# GRADO EN COMERCIO

## TRABAJO FIN DE GRADO

## "IA y el Metaverso: aspectos jurídicos"

IVÁN DOMINGO CÁRDABA

**FACULTAD DE COMERCIO VALLADOLID,**
**22/07/2024**

FACULTAD DE COMERCIO
Universidad de Valladolid

FACULTAD DE COMERCIO
Universidad de Valladolid

# UNIVERSIDAD DE VALLADOLID

# GRADO EN COMERCIO

CURSO ACADÉMICO 2023/2024

## TRABAJO FIN DE GRADO

## "IA y el Metaverso: aspectos jurídicos"

**Trabajo presentado por: Iván Domingo Cárdaba**

**Tutor: José Miguel Hernández-Rico Bartolomé**

**FACULTAD DE COMERCIO**
Valladolid, 22/07/2024

# ÍNDICE

# 1. INTRODUCCIÓN

Cada revolución a lo largo de la historia humana ha provocado cambios en los códigos de conducta de la sociedad. En la era actual, marcada por la revolución de internet y los dispositivos digitales, presenciamos un avance tecnológico tan vertiginoso y exponencial que podría parecer desafiante adaptarse a él.

El ámbito legal, consciente de esta acelerada revolución, ha comenzado a regularla para establecer límites a su crecimiento. Hace tan solo cuarenta años, que apareció "ENIAC" (el primer ordenador del mundo). Posteriormente surgió Internet (1983), permitiéndonos buscar cualquier información simplemente tecleando y ahorrándonos buscar en las pesadas y gigantes enciclopedias. A continuación, en el 1996, Google entró en escena, a partir de aquí es cuando comienza el ya citado crecimiento exponencial, dado que en el año 2002 se publica en España la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El siguiente paso, fueron las redes sociales como Facebook y Twitter, las cuales conocemos ahora y están ya "controladas" por las regulaciones actuales, pero sin dejar descanso alguno a los investigadores y desarrolladores de software (conjunto de programas e información con la que trabaja el ordenador), ya que actualmente se encuentran desarrollando dos nuevas formas, a priori, de mejorar el día a día. Estas dos tecnologías son la Inteligencia Artificial y el Metaverso. En el caso de la primera, ésta es capaz de generar contenido y pensar por sí misma.

En este trabajo analizará hasta qué punto su contenido es lícito, sus creaciones presentan originalidad y, por lo tanto, se las podrá "adueñar" esta tecnología o si por el contrario, toda la responsabilidad recaerá sobre aquellos que le dan las instrucciones y los que la entrenan. También se analizará qué tipos de datos han sido utilizados para su entrenamiento y sí su "recolección" ha sido legítima o no, para así ser capaces de comprobar cómo las autoridades se están encargando de regular toda esta revolución tecnológica.

En lo que respecta al Metaverso es un reto aún mayor, dado que se trata de un universo virtual que ha de ser regulado prácticamente desde cero. En cuanto a los desafíos que se hacen presentes ante este "universo paralelo", estos se basan en puntos clave, como la protección del usuario, la propiedad privada que pueda presentar cada usuario tras la compra del terreno, la protección de sus datos personales y cómo éstos están siendo utilizados. Planteándonos retos adicionales en términos de protección de usuarios, propiedad privada, manejo de datos personales y regulación de posibles ciberdelitos.

Teniendo como finalidad de este trabajo estudiar el estado en el que se encuentran las regulaciones en este momento, analizando el marco jurídico tanto de la Inteligencia Artificial como del Metaverso y de los contratos inteligentes, tratando de buscar puntos débiles y proponer ideas para que sean añadidas o tomadas en consideración, para su posterior aplicación en la regulación vigente.

Hay que puntualizar que al tratarse de un tema novedoso como es la Inteligencia Artificial y el Metaverso, será necesario definir los conceptos claves que resultarán necesarios para el correcto entendimiento del trabajo.

# 2. MARCO TEÓRICO

El término de Inteligencia Artificial (IA a partir de ahora) fue acuñado en el año 1940, cuando los matemáticos Norbet Wiener y John Von Neuman sentaron las bases de la IA en su teoría de sistemas y computación. Sin embargo, no fue hasta el año 1956 que John McCarthy durante una conferencia en la Universidad de Dartmouth, formalizó y definió el concepto de la siguiente manera, "la ciencia y la ingeniería de hacer máquinas inteligentes, especialmente programas de computadora inteligentes" (Gobierno de España, Plan de Recuperación, Transformación y resiliencia, 2023).

Para que la IA opere de manera óptima, será indispensable contar con una interfaz de usuario que facilite su utilización por parte del usuario, dado que este es el espacio donde se produce la interacción entre el usuario y la máquina. Además, es fundamental entrenar a la IA mediante el aprendizaje automático, una rama de la inteligencia artificial se enfoca en la implementación de métodos tales como el aprendizaje supervisado, no supervisado, semisupervisado, por refuerzo, profundo, activo, federado, incremental y basado en instancias. Estos métodos permiten que las máquinas aprendan a partir de datos y experiencias previas, sin la necesidad de programarlas individualmente para cada tarea específica.

Aprendizaje supervisado o “machine learning” es la técnica que busca entrenar al sistema de Inteligencia Artificial mediante un conjunto de datos etiquetados, (datos que han sido tratados previamente para obtener un resultado específico) para cumplir con un objetivo concreto.

Aprendizaje no supervisado aquel método de aprendizaje que hace uso de datos no etiquetados (datos que no han sido tratados previamente) y del conjunto de reglas y procesos diseñados para permitir que una máquina pueda aprender (de aquí en adelante algoritmos) para analizar y agrupar datos sin la intervención humana.

Aprendizaje semisupervisado, técnica de aprendizaje que hace uso de un conjunto de datos seleccionados, no seleccionados y algoritmos mejorando así los resultados del sistema.

Aprendizaje por refuerzo es el método de entrenamiento basado en el prueba y error.

Aprendizaje profundo o red neuronal, modelo de aprendizaje inspirado en el funcionamiento del cerebro humano. Se encuentran compuestas por una serie de

"nodos" (unidad fundamental que simula una neurona humana pudiendo enviar o recibir información) interconectados, conocidos como "neuronas artificiales" o "unidades". Estas neuronas artificiales crean un sistema adaptable de capas aprendiendo de sus errores dando lugar a distintos tipos de disposiciones neuronales.

Red neuronal Profunda, modelo de red neuronal artificial compuesta por múltiples capas intermedias entre la cola de entrada y la capa de salida. Éstas permiten a la red resolver problemas complejos.

Red neuronal convolucionales, redes neuronales diseñadas específicamente con el fin de procesar datos estructurados en forma de mallas. Este método de gestión de datos basado en la descentralización tanto de la responsabilidad como de los datos de almacenaje. Estas redes se encuentran diseñadas para las tareas de visión por ordenador como la clasificación de imágenes.

Red neuronal recurrente, conjunto de conexiones neuronales que permiten la memorización y el procesamiento de datos dentro de una estructura en bucle, repitiendo una serie de órdenes las veces necesaria.

Red generativa adversativa, es un enfoque de entrenamiento que implica la competencia entre dos redes neuronales. Una de las redes se encarga de generar datos falsos y desorganizados, lo cual obliga a la segunda red, a través de un proceso de discriminación[1], a identificar y seleccionar los datos reales. Este tipo de red se fundamenta en los principios del modelo de difusión, técnica que consiste en introducir y eliminar ruido[2] en los datos procesados.

Modelo basado en transformadores, hace referencia a redes neuronales que adquieren el contexto y el significado al relacionar datos secuenciales de manera efectiva.

[1] Toma de decisiones que afecta a las personas.

[2] Información inexacta o irrelevante que interfiere en la comprensión de los datos por parte de los algoritmos.

Autocodificadores Variacionales, tipo red neuronal enfocado en la generación de representaciones latentes (espacio donde encuentran los datos que serán utilizados) eficientes.

Aprendizaje federado, modelo de entrenamiento basado en una arquitectura descentralizada formada por diversos dispositivos.

Aprendizaje basado en instancias, este método se basa en el uso de algoritmos con datos etiquetados y métricas de similaridad[3].

Dada la ambigüedad en la especificación de los tipos de IA existentes, se han propuesto diversas clasificaciones basadas en criterios individuales. Arend Hintze establece una clasificación que se fundamenta en la capacidad predictiva y el nivel de complejidad que puede llegar a presentar una máquina. Por su parte, Stuar Russell y Peter Norving, optaron por clasificar estos sistemas según la capacidad de razonamiento. Otra de las clasificaciones más importante se centra en el nivel de inteligencia. Adicionalmente, se considera una clasificación basada en el nivel de riesgo asociado a los sistemas de inteligencia artificial. Para finalizar, encontramos la clasificación por tipo de código teniendo que distinguir entre código abierto o cerrado.

**Clasificación de Arend Hintze**

En primer lugar, las máquinas reactivas son aquellas que hacen uso de la inteligencia artificial, aunque no son capaces de recordar experiencias claves el ejemplo más conocido es el de Siri la asistente de Apple.

En segundo lugar, se encuentran las máquinas con memoria limitada, la diferencia respecto a las máquinas anteriores estas sí que presentan memoria de los aprendizajes, aunque por un corto periodo de tiempo.

La siguiente máquina que nombra Hintzer son las máquinas que aplican la teoría de la mente. Éstas procesan emociones y realizan reflexiones como si de un humano se tratara.

En último lugar, las máquinas de autoconciencia buscan no sólo comprender las emociones si no tener las suyas propias.

[3] Reglas para encontrar el parecido entre dos fragmentos de información.

**Clasificación de Stuart Russell y Peter Norving**

En primera instancia, los autores definen los sistemas que piensan como humanos refiriéndose a aquellos sistemas que tienen como finalidad imitar el pensamiento humano.

En el siguiente nivel encontramos a los sistemas que actúan como humanos centrándose en cómo actúa el sistema, no en cómo piensa.

El tercer lugar es para los sistemas que piensan racionalmente. Estos buscan diseñar el sistema de manera que sea capaz de percibir, razonar y actuar como si fuera una persona.

Por último, los sistemas que actúan racionalmente son aquellos que buscan imitar al ser humano en su totalidad.

**Clasificación por nivel de inteligencia**

Esta clasificación se inicia con la superinteligencia artificial, definiéndose como aquella Inteligencia Artificial capaz de superar las capacidades cognitivas humanas ya sea de manera global, específica, creativa, ética o socialmente según el enfoque dado al sistema. Actualmente, esta superinteligencia es considerada una hipótesis meramente teórica, dado que resulta imposible desarrollar sistemas con este nivel de conciencia.

En segundo lugar, se encuentran las Inteligencias Artificiales generales o fuertes, cuyo propósito es la creación de un sistema que iguale o supere la inteligencia humana. Estas se basan en redes neuronales, en la lógica y el razonamiento, en métodos de aprendizaje continuo, en sistemas multiagente y modelos cognitivos.

Basadas en redes neuronales, hacen uso de las redes neuronales para aprender y adaptarse

Basadas en lógica se centra en el uso de los modelos lógicos para tomar sus decisiones.

Basadas en métodos de aprendizaje continuo presenta la capacidad de aprender de manera continua y así adaptarse a las situaciones de manera autónoma.

Basadas en modelos cognitivos integran modelos cognitivos imitando las capacidades cognitivas humanas.

El siguiente paso en la clasificación de la inteligencia artificial es la IA generativa, que abarca sistemas capaces de crear contenido multimedia, como música, videos e

imágenes. Además, estos sistemas pueden mostrar creatividad, posicionándose en un punto intermedio entre la IA débil y la IA general. La IA generativa opera a través de redes generativas adversarias, modelos de difusión, modelos basados en transformadores y autocodificadores variacionales. Gracias a estas tecnologías de IA generativa, empresas como Google han logrado desarrollar modelos como Gemini e integrarlos en sus aplicaciones, como su motor de búsqueda.

En último lugar se encuentran las IA estrechas o débiles, estos sistemas se enfocan en la realización de tareas específicas superando así al ser humano como por ejemplo "Siri" (la asistente de Apple). Este tipo de Inteligencia Artificial presenta diversas subdivisiones basadas en su uso personal.

Primero, encontramos los sistemas de recomendación utilizados en plataformas como Amazon para ofrecer recomendaciones personalizadas a los usuarios.

En segundo lugar, se destaca el procesamiento de lenguaje natural, una disciplina de la Inteligencia Artificial enfocada en la interacción entre ordenadores y el lenguaje humano, necesitando desarrollar softwares capaces de entender, interpretar y replicar el lenguaje humano como en los chatbots (como ChatGPT).

Avanzando con la clasificación, surge la visión por ordenador, un campo de la Inteligencia Artificial que se dedica al desarrollo de softwares capaz de comprender e interpretar imágenes mediante el empleo de algoritmos y redes neuronales.

En último lugar, el reconocimiento de voz está relacionado con la tecnología que permite a los sistemas informáticos interpretar y convertir la voz humana en texto.

**Clasificación según su riesgo**

La clasificación de las inteligencias artificiales según el riesgo asociado a su implementación y aplicaciones se dividen en diferentes tipos basados en las posibles consecuencias y desafíos éticos y legales que presentan. Estas categorías incluyen IA de bajo riesgo o nulo, medio o limitado y alto.

Sistemas de riesgo bajo o nulo, aquellos sistemas que no presentan un riesgo significativo para los individuos o la sociedad en general. Estos sistemas suelen estar relacionados con tareas simples y de baja complejidad, donde las posibles consecuencias

negativas son limitadas, como los asistentes de servicio al cliente o los filtros de spam del correo electrónico.

Sistemas de riesgo medio o limitado, pueden tener implicaciones más significativas y complejas en comparación con las de bajo riesgo. Estos sistemas pueden involucrar la toma de decisiones críticas o la interacción con datos sensibles que requieren supervisión y control. En este contexto, se aprecian los sistemas de recomendación de crédito, análisis predictivo en atención médica o sistemas de videovigilancia.

Sistemas de alto riesgo, tienen la capacidad de generar impactos significativos en individuos, organizaciones o en la sociedad en su conjunto. Este tipo de IA está obligado a cumplir con requisitos específicos, especialmente cuando se utiliza como componente de seguridad en un producto o está sujeto a la legislación de la Unión Europea. Dentro de esta clasificación se encuentran sistemas de identificación biométrica, infraestructuras críticas, educación y formación profesional, empleo, acceso y disfrute de los servicios públicos y privados esenciales, fuerzas y cuerpos de seguridad, gestión de la migración, así como la administración de justicia y procesos democráticos.

Sistema de identificación biométrica, hace referencia al uso de características físicas o comportamentales únicas de un individuo. En el marco de la Inteligencia Artificial, se emplea en sistemas de identificación biométrica con el propósito de mejorar la precisión y la eficiencia en la autenticación de personas.

Sistema de infraestructuras críticas, este involucra sistemas y activos fundamentales para el funcionamiento de la sociedad, como sistemas energéticos, de agua, transporte, comunicaciones y finanzas. La IA se aplica en la gestión y protección de estas infraestructuras críticas con el fin de mejorar la eficiencia, la seguridad y la respuesta ante posibles amenazas o incidentes.

Sistemas de educación y formación profesional, se utilizan para personalizar el aprendizaje, proporcionar recomendaciones educativas, automatizar tareas administrativas y facilitar la formación profesional continua.

Sistema de empleo, se emplea en la gestión de recursos humanos y la evaluación del desempeño laboral.

Sistemas de acceso a los servicios públicos y privados esenciales se busca mejorar la accesibilidad a servicios fundamentales como la atención médica, el transporte público o los servicios gubernamentales.

Sistemas de fuerzas y cuerpos de seguridad se utilizan en sistemas de videovigilancia, análisis de datos y la identificación de patrones delictivos.

Sistemas de gestión de la migración se emplean en la gestión de fronteras, el control de pasaportes y la detección de fraudes

Sistemas de administración de justicia y procesos democráticos, se aplican en la optimización de procesos legales, la identificación de tendencias dentro del sistema judicial y la gestión de documentos legales. Además, estos sistemas tienen el potencial de fortalecer los procesos democráticos mediante la promoción de la transparencia, la eficiencia y la accesibilidad en el funcionamiento de las instituciones legales y democráticas.

Es esencial tener en cuenta la manera en que se emplean los datos en el desarrollo de sistemas de Inteligencia Artificial, garantizando así el respeto a los derechos y la privacidad de las personas. Asimismo, se debe asegurar la equidad y transparencias en los algoritmos.

La ética en la IA abarca una diversidad de aspectos, incluidos la privacidad y la protección de datos, los sesgos algorítmicos, la responsabilidad y transparencia, el impacto en el empleo y la sociedad y la seguridad y el riesgo.

En el caso de los sesgos en la IA, se refiere a la aparición de resultados distorsionados debido a prejuicios humanos que afectan a los datos de entrenamiento. Los diferentes tipos de sesgos incluyen:

Sesgo de selección de datos, conjunto de datos utilizado en el entrenamiento del algoritmo de la IA que no es representativo con la población.

Sesgo de confirmación, se refiere a la inclinación de los sistemas de inteligencia artificial a favorecer decisiones que refuerzan prejuicios existentes o estereotipos fundamentados en datos objetivos. Un ejemplo hipotético sería un escenario en el que un sistema establece los intereses de acuerdo con un grupo demográfico específico, en lugar de considerar criterios objetivos e imparciales.

Sesgo de similitud, se manifiesta cuando el algoritmo toma decisiones basadas en la similitud con otro conjunto de datos, lo que restringe la amplitud de la decisión adoptada. Un ejemplo significativo de este fenómeno se produciría cuando un sistema de empleo sugiriese puestos de trabajos similares a los desempeñados previamente por un candidato, reduciendo de manera significativa las oportunidades disponibles.

Sesgo de etiquetado, surge cuando las etiquetas asignadas a los datos empleados en el entrenamiento de la IA reflejan prejuicios humanos. Un caso ilustrativo de este fenómeno es el reciente incidente relacionado con la inteligencia

artificial de Google, que ha sido objeto de controversia en las redes sociales debido a la presencia de este sesgo en sus resultados.

Sesgo de atención, se da en el momento que los algoritmos de la IA otorgan mayor importancia a unos atributos que a otros. Un ejemplo hipotético sería si en un proceso de contratación automatizado se centrara únicamente en la experiencia laboral previa, dejando a un lado otras cualidades relevantes.

Sesgo temporal, se manifiesta cuando se entrena al algoritmo utilizando datos que reflejan desequilibrios históricos o tendencias pasadas.

En otro orden de ideas, resulta esencial identificar a los participantes a lo largo de la cadena de responsabilidades, entre los cuales se incluyen los desarrolladores de algoritmos, proveedores de datos, usuarios y operadores, productores de hardware (parte física de un equipo informático) y la empresa propietaria.

Desarrolladores del Algoritmo, engloba a los ingenieros y científicos que elaborar los códigos, considerandolos responsables en caso de que los sistemas creados por ellos presentan deficiencias.

Proveedores de datos, por su parte, asumen responsabilidad en caso de que se produzca algún daño derivado de sesgos incorporados en los datos utilizados para el entrenamiento de las inteligencias artificiales

Usuarios y Operadores, también tienen responsabilidad en caso de utilizar la herramienta de manera negligente.

Fabricantes de hardware, aquellos que forman parte de esta cadena de responsabilidades son considerados responsables en situaciones en las que los fallos estén vinculados al hardware que sustenta el software de la inteligencia artificial.

Empresa propietaria que se beneficiaria de la IA, debe responder como responsable en caso de no cumplir con las prácticas recomendadas y las regulaciones establecidas para su uso adecuado.

Es fundamental resaltar que, con el propósito de identificar el momento en que se produce un problema y atribuir la responsabilidad correspondiente, surge el concepto de “caja negra”, similar al utilizado en la aeronáutica. Este dispositivo registra todas las acciones llevadas a cabo dentro del sistema de inteligencia artificial.

**Definiciones del Metaverso**

Un concepto esencial para comprender el Metaverso es el de cadena de bloque o "blockchain", una tecnología basada en sistemas descentralizados y distribuidos que facilita el intercambio seguro de información y activos digitales, a través de una red de nodos[4] interconectados. Sus características principales incluyen bloques, la criptografía, los contratos inteligentes, tokens y tipos de blockchain.

En primera instancia, se requiere un análisis detallado de los bloques y las cadenas que conforman la blockchain. Los bloques tienen la función de almacenar información relativa a transacciones encadenadas en una secuencia, lo que da lugar a la creación de una cadena inmutable, es decir, que no puede modificarse. Existen diversas categorías de bloques basados en funcionalidad, estructura, tamaño, cadena o en estado.

Los bloques de transacciones contienen detalles sobre las acciones realizadas, como la cantidad de activos transferido y las direcciones de origen y destino. Por otro lado, los bloques de contratos inteligentes almacenan información relacionada con la ejecución de contratos, incluyendo condiciones y acciones automáticas a realizar. Además, los bloques de datos pueden contener información no transaccional o metadatos (datos que describen a otros datos) para la identificación de la propiedad de los activos digitales o datos de votación. Respecto a los tipos de blockchain, encontramos públicas, privadas, de consorcio, híbridas, automatizadas, autorizadas y sin permisos.

Blockchain pública, se caracteriza por no requerir permisos para unirse y pudiendo validar las transacciones, así como leer y escribir en la cadena de bloques.

Blockchain privada, se restringen los permisos de entrada y validación a un grupo específico de entidades.

Blockchain de consorcio, cambian las dos cadenas anteriores dado que varios participantes controlan la validación de las transacciones, compartiendo la responsabilidad entre los miembros del consorcio.

Blockchain híbrida, aprovecha los puntos fuertes de las cadenas públicas y privadas.

[4] Red de ordenadores que ejecutan de manera conjunta el software de la blockchain.

Continuando con la blockchain, la criptografía representa la vertiente de la criptología que se dedica a la generación de códigos destinados a encriptar el contenido del mensaje, volviéndolo ininteligible para aquellos que carecen de la clave correspondiente. En virtud de esta premisa, resulta imperativo que la blockchain integre la criptografía a fin de alcanzar tales metas como la garantía de transacciones seguras, la preservación de la privacidad, la invariabilidad de los datos y la seguridad en los accesos.

En lo que respecta a los tokens estos son una unidad criptográfica emitida por una entidad dentro de la blockcahin y se clasifican en dos categorías distintas: los tokens fungibles y los tokens no fungibles. En el caso de los tokens fungibles, exhiben atributos tales como la intercambiabilidad, donde el valor de cada token es igual para aquellos que pertenecen a la misma forma y clase, y la divisibilidad, puesto que pueden fraccionarse en unidades sin menoscabar su valor. Un ejemplo de esta categoría lo constituyen las criptomonedas como Bitcoin.

Por su parte, los tokens no fungibles (NFTs) exhiben rasgos opuestos a los tokens fungible. En términos de singularidad, cada NFT es único y presenta atributos distintivos que lo diferencian del resto, además de contar con un identificador exclusivo. En cuanto a su divisibilidad, estos activos son indivisibles, lo que implica que no pueden fraccionarse en partes. Otra característica relevante es la propiedad, ya que los NFTs representan derechos exclusivos sobre activos digitales, como obras de arte o propiedades virtuales, lo que condiciona su escasez al emitirse cantidades limitadas. Los NFTs abarcan una amplia gama de aplicaciones desde el arte digital hasta los juegos, propiedades virtuales en el Metaverso, música, entretenimiento y otros materiales de creación propia. Adicionalmente, los NFTs tienen aplicaciones de utilidad como la autenticación y certificación de productos de lujo y obras de artes físicas. Otro tipo de NFT es el que se centra en las experiencias y entradas a eventos virtuales, permitiendo a los usuarios participar en eventos exclusivos en el espacio digital, así como los certificados y credenciales digitales tokenizados que representa logros como lo sería un título académico o credenciales certificadas.

En tercer lugar, los contratos inteligentes o “smartcontracts” son aquellos programas informáticos ejecutados en la blockchain que incorporan características como la automatización, permitiendo su ejecución inmediata una vez se cumplan las condiciones programadas. Esta automatización prescinde de intermediarios, lo que los hace más rápidos, eficientes y transparentes en las transacciones, que pueden certificarse en la blockchain. La seguridad de los contratos inteligentes se basa en la criptografía, asegurando su inmutabilidad para prevenir fraudes y garantizar que las partes cumplan con los términos del acuerdo. Estos contratos encuentran aplicaciones en las finanzas

descentralizadas (DeFi) facilitando los préstamos y otras operaciones financieras, así como en la gobernanza descentralizada facilitando a los titulares de los tokens participen en la toma de decisiones en protocolos y organizaciones descentralizadas. La de datos también son una parte fundamental de los contratos inteligentes ya que permite que los contratos inteligentes interactúen con los datos del mundo real. La provisión de datos es esencial para la funcionalidad de los contratos inteligentes, ya que les permite interactuar con la información del mundo real. Ethereum es conocida por su capacidad para la ejecución de smartcotracts a través de su blockchain.

El nacimiento del Metaverso se remonta a 1938, cuando el poeta francés Antonin Artaud acuño el término de "realidad virtual" en su obra "El teatro y su doble". Posteriormente, en 1982 con la película de "Tron". No obstante, fue en 1992 cuando Neal Stephenson introdujo el concepto de "Metaverso" en su novela "Snow Crash" describiéndolo como un multiverso virtual donde los usuarios podrían interactuar y explorar por una infinidad de mundos digitales.

En 2003 se lanzó al mercado un mundo virtual "Second Life", que permitía a los usarios crear mundos virtuales, interactuar con ellos e intercambian bienes virtuales. Tan solo tres años después del lanzamiento de Second Life, se introdujo "Roblox", una plataforma centrada en facilitar al usuario la creación de mundos virtuales. En 2012, surgieron proyectos innovadores como "Oculus Rift", un casco 3D inmersivo que permite al usuario reproducir una experiencia virtual como si fuese real. Esto provocó una revolución tecnológica y atrajo el interés de las desarrolladoras de videojuegos en la realidad aumentada, como fue el caso Niantic con el lanzamiento de "Pokemon Go", un juego basado en la realidad aumentada que fusiona el mundo ficticio de los Pokémon con el mundo real.

A pesar del desarrollo continuo del Metaverso, su definición no del todo clara. Podría entenderse como una red constituida por un conjunto de entornos digitales que, gracias a la integración de tecnologías como la realidad virtual, la realidad aumentada y la "blockchain", crean un nuevo universo.

Si queremos entender el funcionamiento del Metaverso se deben los tipos de datos que lo componen, estos son:

Datos dinámicos, son los encargados de generar una experiencia personalizada a los usuarios ya que nos permite que el entorno cambie a medida que interactuamos con él.

Datos estructurales, aquella información que permite funcionar al Metaverso.

Datos omniversales, es toda información captada por entidades externas dentro del Metaverso.

Datos secuenciales, es aquella información que se guarda de manera organizada de manera lineal.

Por otro lado, en el contexto del Metaverso conceptos como los gemelos digitales son indispensables, ya que implican la recreación digital de objetos físicos en un entorno virtual. Otro concepto de vital importancia es el de avatar virtual siendo una representación visual de nuestra propia persona física dentro de los entornos virtuales pudiendo ser realistas si estos se asemejan a la apariencia física, estilizados si son representaciones simplificadas o caricaturizadas, no humanos si estas representan criaturas o animales, y personalizables si el usuario es capaz de modificar la apariencia, la ropa, los accesorios y la personalidad.

En el caso de los entornos digitales se hace referencia a todas las plataformas creadas mediante tecnología digital como una página web o una aplicación móvil. En el caso de los entornos virtuales, estos tienen como objetivo replicar o simular experiencias 3D con la cual los usuarios pueden interactuar. Los entornos virtuales pueden ser divididos según su propósito, su tecnología, su grado de inmersión, su interactividad y su nivel de centralización.

**Clasificación según su propósito**

Entornos de entretenimiento, diseñados para el ocio y la diversión como videojuegos en línea.

Entornos educativos, creados para la enseñanza, por ejemplo, los simuladores de laboratorio como (Labster).

Entornos de trabajo y colaboración, facilitando la colaboración y la productividad entre equipos que trabajan en remoto. Un ejemplo de esto es Microsoft Horizon que permite entrar al ordenador de manera remota.

Entornos sociales, espacios de interacción social como VRChat que permite interactuar con otros usuarios.

Entornos de comercio y negocios, permiten la compra y la venta de bienes y servicios virtuales como Amazon VR.

Entornos jurídicos, espacio donde se administran y aplican normativas legales, se llevan a cabo transacciones legales y se proporciona asesoramiento. En estos entornos se incluyen los tribunales virtuales utilizados mayoritariamente en China y operan de forma similar a los tribunales físicos. Asimismo, se destacan los arbitrajes virtuales, los cuales constituyen un mecanismo alternativo de resolución de conflictos donde dos o más individuos optan por resolver una disputa surgida en el ámbito del comercio electrónico.

**Según su tecnología**

Realidad virtual (RV), entorno creado por escenas y objetos digitales que presentan una imagen realista creando la sensación de encontrarse inmerso en ese lugar. Las principales aplicaciones que encontramos haciendo uso de esta tecnología serían “Oculus Ritf”, “PlayStation VR”. Cabe destacar que dentro de la realidad virtual se hacen presentes aplicaciones especializadas como es el caso de “Legal Specch VR”, idea galardonada por la Fundación Mutualidad Abogacía en el año 2020 gracias al proyecto presentado. Este software se basa en simular juicios mediante el uso de esta tecnología.

Realidad aumentada (AR), experiencia interactiva creada mediante un equipo informático con el objetivo de mejorar la interacción perceptual con el mundo real mediante el uso de Hardware como las “Apple Vision Pro” y de un software como “JigSpace”.

Realidad mixta (MR), fusión de elementos virtuales y reales permitiendo al usuario la interacción en tiempo real.

Entornos basados en blockchain, se basa en la tecnología blockchain para la gestión de activos y la economía digital en el entorno digital.

**Según su nivel de centralización**

Entornos virtuales centralizados, se caracterizan por presentar un control y propiedad centralizada a manos d una única organización o empresa imponiendo esta sus reglas a los usuarios. Un ejemplo sobre estos entornos es Meta (la antigua Facebook).

Entornos virtuales descentralizados, nacieron con el objetivo de ser gestionados por los usuarios mediante una forma de organización conocida como organización autónoma descentralizada (DAO) en la que los usuarios que hayan invertido

dinero en el desarrollo tienen capacidad de asistir a la asamblea y así tomar decisiones de manera democrática.

Habiendo terminado de analizar los entornos digitales entramos en la web 3.0 la cual se centra en la descentralización de los datos, la privacidad del usuario, la interoperabilidad de las plataformas y la utilización de tecnologías como inteligencia artificial, blockchain, realidad aumentada y realidad virtual para ofrecer una mejor experiencia web. El objetivo de esta evolución de la web es el de proveer a los usuarios un mayor control sobre sus propios datos y que pueden interactuar de forma segura por internet sin depender de los intermediarios centralizados. Para su correcto funcionamiento, la blockchain es fundamental ya que permite las transacciones seguras y transparente, así como la creación de aplicaciones descentralizas (dApps). Estas son un tipo de aplicación ejecutada mediante una red descentralizada, como la blockchain y que hacen uso de los contratos inteligentes como por ejemplo las finanzas, la identidad, los mercados descentralizados donde se facilitan los intercambios de bienes y servicios gracias a la ausencia de intermediario.

Otra de las actualizaciones que incorpora el Metaverso a internet es la web 3D, la cual hace que los contenidos y experiencias en internet se basen en entornos tridimensional permitiendo a los usuarios explorar y experimentar de los entornos digitales mediante el uso de la realidad virtual y aumentada haciendo que por ejemplo el usuario pueda visitar una tienda en tiempo real desde su casa gracias a los sensores de realidad virtual y se pruebe la ropa en un espejo virtual.

**Definiciones Jurídicas**

Tras un exhaustivo análisis de los conceptos fundamentales relacionados con la Inteligencia artificial y el Metaverso desde una perspectiva conceptual, es imperativo abordar estos temas desde un punto de vista jurídico. En este sentido, es crucial definir los conceptos esenciales que rigen las normativas y que regulan estas áreas como los guardianes de acceso o “gatekeepers” y los proveedores, entre otros.

Guardianes de acceso o “gatekeepers”, entidad o individuo encargado de controlar el acceso a información, servicios o sistemas. En el contexto de la IA, un guardián de acceso es indispensable para la supervisión del flujo de datos, la validación de entras y salidas y la implementación de políticas de acceso.

Proveedor, se refiere a las personas físicas o jurídicas que suministran productos, servicios o tecnologías a otras entidades. En el ámbito de la inteligencia artificial,

los proveedores pueden ser responsables del desarrollo, entrega y soporte de soluciones de IA y recursos tecnológicos necesarios para su funcionamiento.

Distribuidor, intermediarios que comercializan y distribuyen productos o servicios a los consumidores finales o a otras entidades comerciales. En el contexto de la inteligencia artificial, los distribuidores pueden gestionar la entrega y venta de sistemas de IA y soluciones tecnológicas asociadas.

Importador, persona física o jurídica que introduce productos, tecnologías o servicios desde un país extranjero con el propósito de comercializarlos, utilizarlos o distribuirlos en el mercado local. En el ámbito de la inteligencia artificial, los importadores son responsables de garantizar el cumplimiento de las normativas locales y la calidad de los productos importados.

Responsable del despliegue, persona o entidad encargada de la implementación y gestión operativa de sistemas de inteligencia artificial en un entorno específico. Su labor incluye asegurar el correcto funcionamiento, supervisión y mantenimiento del sistema desplegado.

Operador, individuo o entidad que maneja y controla directamente el funcionamiento de un sistema o tecnología específica. En el contexto de la inteligencia artificial, los operadores son responsables de la gestión diaria de las aplicaciones de IA y su interacción con los usuarios.

Responsable autorizado, persona o entidad legalmente designada para supervisar y garantizar el cumplimiento de regulaciones y normativas relacionadas con el uso y desarrollo de tecnologías o servicios. En el ámbito de la inteligencia artificial, el responsable autorizado puede supervisar que los sistemas de IA operen de acuerdo con los estándares de cumplimiento y seguridad establecidos.

Autoridad notificante, organismo o entidad oficial encargada de recibir notificaciones y controlar determinados aspectos regulatorios en una jurisdicción específica. En el contexto de la inteligencia artificial, la autoridad notificante puede ser responsable de captar informes sobre el uso, condiciones de riesgo y la implementación de sistemas de IA.

Practicas IA prohibidas, conjunto de actividades, técnicas y métodos de inteligencia artificial que están explícitamente prohibidos por razones éticas, de seguridad, legales o de protección de derechos. En el ámbito del metaverso, esto también incluye prácticas que explotan la realidad virtual o aumentada de manera inapropiada o perjudicial,

como por ejemplo la discriminación algorítmica intencionada o la exploración no consentida de datos privados.

Técnicas subliminales, métodos que emplean señales o estímulos por debajo del umbral de percepción consciente para influenciar y dirigir el comportamiento de las personas sin su conocimiento o consentimiento explícito. En el ámbito de la inteligencia artificial, el uso de técnicas subliminales para manipular o influenciar decisiones está considerado una práctica prohibida y altamente regulada como por ejemplo la manipulación o la publicidad subliminales.

Minimización de datos, principio que establece el modo de recopilación y procesamiento de datos personales que sean estrictamente necesarios para el propósito que han recolectado. En el ámbito de la inteligencia artificial y el Metaverso, este principio implica que las plataformas y aplicaciones solo deben solicitar y utilizar la información personal absolutamente indispensable para las funcionalidades ofrecidas.

Limitación de la finalidad, establece que los datos solo deben ser recogidos para objetivos específicos y legítimos y no deben ser procesados de manera incompatible con esos propósitos. En el contexto de la IA y el Metaverso, esto significa que si una entidad recolecta datos con el fin de mejorar la experiencia del usuario en un entorno virtual, no debe utilizar estos datos para otros fines distintos sin el consentimiento explícito del usuario.

Licitud, lealtad y transparencia, requiere que los datos sean tratados de manera legal, justa y transparente. Implica que el procesamiento de datos debe ser conforme a la ley, con respeto y equidad hacia los interesados y de forma comprensible para todos. Las plataformas de inteligencia artificial y el Metaverso deben asegurarse de que su procedimiento de recolección y tratamiento de datos cumplan con todas las leyes de protección de datos vigentes.

Limitación del plazo de conservación, los datos no deben ser conservados más tiempo del necesario para los fines que fueron recogidos. En el Metaverso y en las aplicaciones de IA, se deben establecer políticas claras sobre el tiempo que retendrán los datos personales.

Exactitud, los datos personales deben ser exactos y cuando sea necesario, estar actualizados. Se deben tomar todas las medidas razonables para garantizar que los datos inexactos sean borrados o rectificados sin demora. En áreas donde la IA utiliza datos personales para tomar decisiones, tales como la personalización de contenido o las recomendaciones, es esencial que los datos sean precisos.

Gobernanza, conjunto de normas, reglamento, marcos éticos y técnico y mecanismos similares que establecen el desarrollo y despliegue de las tecnologías de IA.

Integridad y confidencialidad, los datos personales deben ser tratados de una manera que garantice una seguridad adecuada, incluida la protección contra el procesamiento no autorizado o ilegal, así como contra la pérdida o destrucción accidental.

Sistema de gestión de riesgos, protocolo de actuación para el control y disminución de los riesgos que pueden presentar los sistemas de IA.

Contenido sintético, son aquellos datos no creados por un ser humano.

Interoperabilidad, capacidad de los sistemas IA para intercambiar datos de forma segura.

Inteligencia artificial de abierto hace referencia a los sistemas cuyo código fuente y recursos están disponibles públicamente.

Al adentrarnos en los conceptos legales asociados a la inteligencia artificial y el Metaverso, surge la importancia de los derechos legales que amparan las creaciones intelectuales, que abarcan desde inversiones hasta obras literarias, artísticas, símbolos, nombres e imágenes utilizadas en actividades comerciales. Estos derechos se erigen con el propósito de fomentar la innovación y la expresión creativa. Dentro de las manifestaciones de la propiedad intelectual, se destacan los derechos de autor, las patentes, los secretos empresariales, las marcas registradas y los diseños industriales.

En el ámbito de la inteligencia artificial y el Metaverso, los derechos de autor conforman un conjunto de normas y principios que protegen las creaciones humanas en las artes y las ciencias. Estos derechos otorgan a los autores facultades exclusivas sobre sus obras permitiéndoles explotarlas de diversas maneras, ya sea económica o moralmente. Respecto a la inteligencia y el Metaverso, los derechos de autor se manifiestan en diversas formas, tales como derechos de paternidad o autoría, integridad, explotación, económica y adaptación.

Derecho de paternidad o autoría, se fundamenta el reconocimiento del creador de una obra, ya sea en contenido generado por inteligencia artificial o en elementos del Metaverso, siendo imperativo determinar de manera precisa la atribución correcta que incluya a los programadores o usuarios involucrados.

Derecho de integridad, este permite al autor oponerse a modificaciones de su obra que puedan menoscabar su reputación. En el contexto del Metaverso, este

principio cobra relevancia en relación con la forma en que se alteran los avatares y los entornos digitales.

Derecho de explotación económica, abarca la reproducción, distribución, comunicación pública y transformación de la obra. En el ámbito de la inteligencia artificial, estas normas establecen directrices sobre la manera en que una obra generada por IA puede ser explotada. Asimismo, en el Metaverso se refiere a la comercialización de objetivos, terrenos y experiencias virtuales.

Derecho de adaptación, faculta la transformación de una obra original en nuevas formas de expresión. En el contexto de la inteligencia artificial, este derecho se aplica a la adaptación del contenido generado por IA a diversos formatos o contextos, mientras que en el Metaverso engloba las modificaciones de elementos virtuales en los distintos entornos disponibles.

En segundo lugar, se encuentran las patentes que representan derechos exclusivos conferidos por el Estado a los inventores, concediéndoles la facultad de excluir a terceros de la fabricación, uso, venta y distribución de esa invención sin su autorización, generalmente por un periodo limitado de 20 años. En el ámbito de la inteligencia artificial y el Metaverso, las patentes de invención, diseño, modelo de utilidad y de invención aplicada emergen como pilares fundamentales.

La Patente de Invención tiene como finalidad principal salvaguardar las creaciones de los inventores. En el ámbito de la Inteligencia Artificial, estas patentes se enfocan en los innovadores algoritmos, protegiendo aquellos algoritmos disruptivos que desempeñan funciones únicas, como los algoritmos de aprendizaje automático. Se busca amparar los métodos innovadores de entrenamiento para la IA, como la creación de redes neuronales que optimicen los tiempos de entrenamiento o mejoren la precisión predictiva. Respecto al Metaverso, las patentes pertinentes abarcan la realidad virtual y aumentada, protegiendo las innovaciones que fortalecen tanto el hardware como el software. Además, merece mención especial la patente de sistemas y plataformas virtuales, dirigida a la protección de las innovaciones en la infraestructura técnica y arquitectónica de las plataformas en el Metaverso. Por último, las patentes enfocadas en las transacciones y pagos virtuales se centran en resguardar los métodos innovadores para llevar a cabo operaciones en los entornos del Metaverso, tales como un método novedoso de criptomoneda diseñado para asegurar transacciones eficientes y seguras en este entorno virtual.

Por otro lado, la Patente de Diseño tiene como objetivo proteger el aspecto ornamental o estético de un objeto utilitario, como las interfaces de usuario (UI) y las

experiencias de usuarios (UX) innovadoras, garantizando la preservación del diseño de la interfaz de usuario para aplicaciones de IA que mejoran la experiencia del usuario, como el diseño de UI para un asistente virtual de IA que facilita la interacción natural y fluida con los usuarios. En el contexto del Metaverso, emergen los diseños de objetos y entornos virtuales que requieren protección del diseño estético, como el diseño de mobiliario virtual destinado a espacios de reunión dentro del Metaverso.

Patentes de Modelo de Utilidad, se fundamentan en la protección de invenciones que tienen una utilidad práctica específica y que permiten mejorar o modificar un objeto existente para solucionar un problema técnico. En el Metaverso, se busca proteger las innovaciones prácticas que faciliten la interacción y navegación en este entorno, como las herramientas de navegación inmersiva.

Patentes de Invención Aplicada protegen el uso novedoso y específico de la inteligencia artificial en diversas industrias y aplicaciones, como un sistema de detección temprana de enfermedades a través del análisis de imágenes médicas.

En tercer lugar, otra de las componentes de la propiedad intelectual son las marcas registradas o "trademarks", las cuales resguardan signos distintivos utilizados para la identificación de productos y servicios de una empresa con el fin de diferenciarlos de la competencia. Estos signos pueden ser un nombre, un logotipo, un eslogan o una identidad visual de avatares virtuales. En el ámbito de la Inteligencia Artificial, nos encontramos con nombres comerciales empleados para identificar productos de IA, ya sea software, hardware o soluciones empresariales (estrategias, tecnologías y herramientas que permiten resolver problemas en una empresa), como, por ejemplo, el software de optimización de procesos de inteligencia artificial "AIOptimizer". En segundo lugar, los logotipos de empresas representan visualmente a una empresa vinculada con la inteligencia artificial. Por último, los eslóganes, que consisten en frases breves o lemas que promocionan plataformas, aplicaciones o servicios de inteligencia artificial, tal como el lema "Just do it" de Nike.

Por otra parte, en el Metaverso nos encontramos con la identidad visual de avatares virtuales, como "VirtualStyle", marca registrada para una línea de ropa virtual destinada a avatares en diversos entornos del Metaverso. Los nombres de los mundos digitales, como "SecondLife", también son considerados como marcas registradas. Asimismo, al igual que en el ámbito de la inteligencia artificial, es necesario proteger los logotipos.

El próximo aspecto para abordar son los diseños industriales, los cuales protegen el diseño estético de productos virtuales y entornos en el Metaverso, otorgando un derecho

exclusivo sobre la apariencia visual de estos productos y entornos, con el propósito de resguardarlos contra la reproducción no autorizada.

Para finalizar el análisis de la propiedad intelectual y sus diversas categorías, nos encontramos con los secretos empresariales. Estos se fundamentan en información confidencial y valiosa que una empresa mantiene en reserva con el propósito de obtener una ventaja competitiva en el mercado. Dichos secretos pueden abarcar fórmulas, procesos, métodos, técnicas, estrategias o algoritmos. Entre los diferentes tipos se incluyen aquellos relacionados con los algoritmos y modelos de aprendizaje automático, datos de entrenamiento sensibles, diseños y entornos virtuales exclusivos, tecnologías de inmersión virtual propietarias y modelos de negocio innovadores. Algoritmos y modelos de aprendizaje automático, se protegen aquellos algoritmos exclusivos de aprendizaje automático y modelos predictivos que brinden ventajas competitivas a la empresa.

Procesos y métodos patentados se refiere a los procedimientos internos y métodos exclusivos de la empresa para el desarrollo, implementación y mantenimiento de la inteligencia artificial.

Diseños y entornos virtuales exclusivos hacen alusión a todos los diseños únicos de escenarios, mundos virtuales y espacios interactivos del Metaverso.

Tecnologías de inmersión virtual exclusivas son tecnologías patentadas o métodos de interacción únicos que mejoran la inmersión en experiencias virtuales.

Modelos de negocio innovadores se refieren a estrategias empresariales y modelos de monetización personalizados que crean valor en los entornos digitales.

Datos de entrenamiento sensibles consisten en conjuntos de datos valiosos y sensibles usados para entrenar los modelos de inteligencia artificial. Preservar la confidencialidad de estos datos de entrenamiento es crucial para evitar la filtración de información privada y mantener la integridad de los modelos. Dentro de estos datos sensibles se hallan datos de salud, información financiera, datos biométricos, datos genéticos, datos de ubicación, información personal identificable, datos confidenciales de la empresa y comunicaciones y datos de interacción.

Datos de salud se refiere a información confidencial como historiales clínicos, diagnósticos, tratamientos y resultados de pruebas médicas que deben protegerse para salvaguardar la privacidad de los pacientes.

Información financiera abarca datos financieros y bancarios sensibles, como números de cuenta, transacciones, historiales de crédito y

otra información confidencial relacionada con la situación financiera de individuos o empresas.

Datos biométricos se basan en características físicas únicas como huellas dactilares, escaneos de retina, reconocimiento facial y otras medidas utilizadas para la identificación personal.

Datos genéticos comprenden información genética individual como secuencias de ADN, marcadores genéticos y datos relacionados con enfermedades heredables.

Datos de ubicación engloban información sobre la ubicación geográfica de usuarios o dispositivos, revelando patrones de comportamiento y rutinas diarias.

Información personal identificable (PII) representa datos únicos que identifican a una persona, como nombres, direcciones o números de seguridad social.

Datos confidenciales de la empresa incluyen información empresarial clasificada como secretos empresariales, estrategias comerciales o datos de investigación.

Comunicaciones y datos de interacción, estas abarcan registros como correos electrónicos, mensajes de texto, archivos de llamadas o interacciones en redes sociales.

Una vez expuesta la propiedad intelectual, procederemos a abordar las licencias, dado que están intrínsecamente vinculadas a estos derechos. Las licencias constituyen el medio jurídico por el cual el titular de los derechos de propiedad intelectual autoriza a terceros a utilizar, reproducir o modificar su obra protegida por derechos de autor, patentes y otras formas de propiedad intelectual, de acuerdo con los términos y condiciones establecidos en el contrato de licencia. Estas licencias influyen en una amplia gama de activos digitales, como las licencias de uso de algoritmos de IA, modelos de aprendizaje automático, software de IA, datos de entrenamiento, uso de espacios virtuales, propiedad virtual o tecnologías de inmersión. En relación con los tipos de licencias, los más destacados son:

Licencia de uso, acuerdo que establece las condiciones de uso de un algoritmo de IA o un entorno digital, detallando los términos de uso y las restricciones legales.

Licencia de distribución, autorización para la distribución de modelos de IA y diseños dentro de entornos virtuales a diferentes usuarios o empresas bajo condiciones específicas.

Licencia de modificación, acuerdo que define la manera en que se puede modificar un modelo de IA y en qué condiciones estas modificaciones pueden ser distribuidas.

Licencia comercial, permite el uso con fines comerciales de productos o servicios basados en la IA y el Metaverso.

Licencia de software propietario, restringe el acceso al código fuente y la modificación de algoritmos de IA y cambios en los entornos virtuales.

Licencia Creative Commons, permite a los desarrolladores de la IA y el Metaverso establecer de forma creativa y personalizada los términos de uso y distribución.

Licencia de uso único, acuerdo que permite acceder y participar en una única experiencia dentro del Metaverso sin posibilidad de transferencia.

Licencia de suscripción, restringe el acceso a entornos virtuales y el uso de sistemas de IA mediante la imposición de una suscripción de pago.

Licencia perpetua, concede acceso ilimitado al Metaverso y al sistema de IA sin restricciones de tiempo.

**Derechos y obligaciones de los Usuarios**

En primer lugar, se abordarán los diversos tipos de derechos existentes, como el derecho de acceso, rectificación, supresión o al olvido, oposición, reclamación o las decisiones automatizadas y elaboración de perfiles.

Derecho de Acceso, este derecho faculta a los usuarios para conocer qué datos personales están siendo procesados, pudiendo solicitar una copia de estos si lo consideran necesario. En el ámbito de la IA y el Metaverso, significa que los usuarios tienen derecho a acceder a la información recopilada sobe ellos, como los datos de interacción en entonos virtuales o el comportamiento en aplicaciones de IA.

Derecho de Rectificación, los interesados tienen la facultad de corregir datos incompletos si así lo desean. En el contexto de las IA y Metaverso, este derecho se

traduce en la posibilidad de corregir información errónea generada por los algoritmos de IA o en perfiles de avatares en entornos digitales.

Derecho de Supresión o Derecho al Olvido, los afectados pueden requerir la eliminación de sus datos personales en circunstancias específicas, como cuando los datos ya no resultan necesarios para los fines que fueron recopilados. En el ámbito de la IA y el Metaverso, esto implica que los usuarios pueden solicitar la eliminación de datos personales que ya no son relevantes, como información histórica de interacciones en entornos virtuales.

Derecho de Oposición, los individuos tienen la posibilidad de oponerse al tratamiento de sus datos por motivos particulares. En lo que respecta a la IA y el Metaverso, este derecho implica que las personas pueden oponerse al uso de ciertos algoritmos o decisiones automatizadas que afecten sus experiencias en entornos digitales.

Derecho de reclamación, los usuarios podrán presentar reclamaciones ante las autoridades de control su consideran que sus derechos han sido infringidos. En el contexto de la IA y el Metaverso, este derecho garantiza que los usuarios puedan hacer valer sus derechos y presentar reclamaciones en caso de anomalías en el tratamiento de sus datos personales, decisiones automatizadas injustas o vulneraciones de privacidad en entornos digitales.

Decisiones Automatizadas y Elaboración de Perfiles, se reconoce el derecho de no ser objeto de decisiones basadas únicamente en procesos automatizados que conlleven consecuencias legales o significativas. En relación con la IA y el Metaverso, esto implica que los usuarios tienen derechos a comprender y cuestionar las decisiones automatizadas que afecten su interacción y experiencia en las plataformas virtuales, así como la elaboración de perfiles que puedan incidir en su privacidad y seguridad en línea.

En segundo lugar, se destacan obligaciones como la responsabilidad proactiva, la responsabilidad legal, la responsabilidad ética, la responsabilidad técnica, la protección de datos desde el diseño y por defecto, el registro de actividades, la evaluación de impacto de protección de datos y el delegado de protección de datos.

Responsabilidad proactiva, las plataformas deben implementar medidas técnicas y organizativas apropiadas para asegurar el correcto procesamiento de datos conforme a lo establecido en el Reglamento General de Protección de Datos (RGPD).

Responsabilidad legal, obligación de responder por las sanciones o decisiones que puedan tener implicaciones legales. En el contexto de la IA y el Metaverso, la responsabilidad legal implica que las organizaciones y los desarrolladores son responsables de cumplir con, la normativa legal vigente en relación con el uso y desarrollo de tecnologías como la IA y las plataformas del Metaverso.

Responsabilidad ética, establece que se debe actuar de manera moralmente correcta y en concordancia con los principios éticos en el desarrollo, implementación y uso de tecnologías. En el ámbito de la IA y el Metaverso, la responsabilidad ética implica considerar las implicaciones éticas de las decisiones y acciones relacionadas con el desarrollo y uso de tecnologías.

Responsabilidad técnica, se refiere a la obligación de garantizar que las tecnologías como la IA y el Metaverso sean desarrolladas, implementadas y mantenidas de manera segura, fiable y eficaz. En el contexto de la IA y el Metaverso, la responsabilidad técnica implica la necesidad de emplear buenas prácticas de diseño, desarrollo y mantenimiento de los sistemas tecnológicos.

Protección de datos desde el diseño y por defecto, los responsables deben integrar principios de privacidad y protección de datos desde las primeras etapas del desarrollo de sistemas de inteligencia artificial y plataformas en el Metaverso.

Registro de actividades de tratamiento, requiere mantener un registro detallado de todas las actividades de tratamiento de datos.

Evaluación de impacto de protección de datos (EIPD), realización de una EIPD es esencial para identificar y mitigar riesgos asociados co n el tratamiento de datos en contextos de alto riesgo, como el uso intensivo de la inteligencia artificial.

Delegado de Protección de Datos (DPO), deberá designarse un DPO en situaciones donde se realice un tratamiento a gran escala de datos sensibles o monitorización sistemática de individuos.

# 3. Régimen jurídico de la IA, el Metaverso y los Contratos Inteligentes

El avance vertiginoso de la tecnología ha generado la necesidad de establecer marcos regulatorios sólidos que aborden cuestiones legales y éticas emergentes en ámbitos como la inteligencia artificial, el Metaverso y los contratos inteligentes.

En el ámbito de la IA, el Metaverso y los contratos inteligentes, cabe destacar que el Reglamento de la Inteligencia Artificial, ha sido publicado el pasado 13 de junio por lo que estamos ante una regulación nueva.

A continuación, se detallan las principales leyes y regulaciones sobre las inteligencias artificiales actualmente vigentes en Europa que afectan a la IA, el Metaverso y los contratos inteligentes:

**Reglamento General de Protección de Datos (RGPD)**

El Reglamento general de Protección de Datos o Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se basa en describir las condiciones y términos de uso que se deberán seguir en el mercado de las IA, el metaverso y los contratos inteligentes.

A la hora de tratar los datos hay que tener claro los principios básicos como el de licitud, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, los cuales fundamentan las bases del reglamento. Estos principios, establecen que el consentimiento para el tratamiento de datos personales deber ser otorgado de forma libre, específica, informada e inequívoca por parte del titular de los datos. Esto significa que las organizaciones deben informar claramente a los individuos sobre cómo se utilizarán sus datos, teniendo que obtener una autorización explícita para dicho tratamiento.

También se establecen los distintos derechos de los usuarios siendo los más importantes los siguientes, derecho de acceso, derecho de rectificación, derecho de supresión o derecho al olvido, derecho de oposición y el derecho de reclamación. Por su parte, los organizadores son responsables de demostrar el cumplimiento con el RGPD, manteniendo registros detallados de sus actividades de procesamiento de datos. Asimismo, se destaca la importancia de la transparencia en el tratamiento de datos, asegurando que los individuos estén informados sobre cómo se usan sus datos personales.

En caso de que se diera una brecha de seguridad que comprometa los datos personales, a las organizaciones deberán notificar a las autoridades pertinentes y a los individuos afectados en un plazo determinado. Esta medida busca garantizar una respuesta rápida y adecuada ante incidentes de seguridad. Para lograr este objetivo se exige a las organizaciones que implementen mediadas adecuadas para proteger los datos personales contra la pérdida, la destrucción, el acceso no autorizado y cualquier forma de tratamiento ilegal.

En ciertas ocasiones, las organizaciones deberán realizar evaluaciones de impacto en la protección de datos para identificar y mitigar los riesgos asociados con el procesamiento de datos personales, especialmente en situaciones de alto riesgo. De cara a mantener unas buenas prácticas de protección de datos algunas organizaciones deberán designar lo que se conoce como delegado de protección de datos (DPO), este actúa como punto de contacto con las autoridades de control y las personas interesadas, y brindar asesoramiento sobre cuestiones de privacidad y protección de datos. Estas evaluaciones al igual que los delegados de protección de datos, no son obligatorias para todos los caos, únicamente son necesarias si el tratamiento puede entrañar un alto riesgo para los derechos y libertades de los usuarios.

En cuanto a las transferencias de datos es importante determinar si son dentro del mercado europeo o si por el contrario serán transferidos a países externos ya que el RGPD establece claramente que, para la transferencia de datos personales fuera de la unión europea, se deberán exigir unas garantías para proteger los datos cuando se transfieran a países que no ofrezcan un nivel adecuado de protección de datos. Esto garantiza que los datos de los ciudadanos europeos estén protegidos independientemente de donde se procesen.

Por último, los periodos de conservación de los datos, únicamente se deben conservar durante el tiempo necesario para cumplir con los fines que fueron recopilados. Además, especifica que las organizaciones deben establecer políticas de retención de datos claras y eliminar la información cuando ya no sea necesaria, contribuyendo así a la minimización de datos y al respeto de la privacidad.

El RGPD, también recoge las sanciones que se impondrán por el incumplimiento de este, dividiéndose en sanciones en graves o muy graves. En el caso de las infracciones graves, la multa ascenderá hasta diez millones de euros o el dos por ciento del volumen de facturación anual, mientras que en las infracciones muy graves la multa asciende hasta los 20 millones de euros o el cuatro por ciento del volumen de facturación anual. Esclarecer que en ambos casos se aplicará el criterio con mayor cuantía.

**Reglamento de servicios digitales**

El Reglamento de servicios digitales (DSA), también conocido como Reglamento (UE) 2022/2065, es una iniciativa de la Unión Europea para regular el comportamiento de las plataformas en línea y los servicios digitales en un entorno cada vez más digitalizado.

El DSA introduce un marco de responsabilidad clara para las plataformas en línea exigiéndoles afrontar una mayor responsabilidad sobre el contenido que alojan y las interacciones que facilitan. Las plataformas deben implementar medidas para garantizar la seguridad y transparencia en sus operaciones, asegurando un entorno online más fiable y controlado para los usuarios. Es por esto por lo que el reglamento busca reforzar la protección de los datos personales en línea, exigiendo a las plataformas digitales cumplir con las normas de privacidad establecidas en el Reglamento de Protección de Datos de la Unión Europea, obligando a las plataformas a garantizar la privacidad de los usuarios y el tratamiento adecuado de sus datos personales. Otro punto clave dentro de este Reglamento es la transparencia de la publicidad en línea, incluyendo la identificación clara del contenido patrocinado y promocionado, buscando proporcionar a los usuarios una comprensión clara de qué contenido está respaldado por terceros y qué es orgánico.

Por otra parte, una de las preocupaciones clave abordada por la DSA es la lucha contra la desinformación, el discurso de odio y otros contenidos perjudiciales en línea. Por ello las plataformas deben tomar medidas proactivas para eliminar o limitar la difusión de este tipo de contenidos, contribuyendo a un entorno en línea más seguro y saludable. Para conseguir esto, el reglamento fomenta una mayor cooperación entre las autoridades reguladoras y las plataformas digitales para supervisar y garantizar el cumplimiento normativo. Esta colaboración busca garantizar que las plataformas cumplan con las regulaciones y protejan los intereses de los usuarios. Así que desde la DSA se proponen medias de cara a abordar los problemas como el acoso en línea, la difusión de información falsa y otros tipos de abuso digital. Estas medidas están diseñadas para proteger a los usuarios de comportamientos perjudiciales y garantizar un ambiente en línea más seguro y respetuoso, estableciendo unas medias para abordar problemas como el acoso en línea, la difusión e información falsa (“fakenews”) y otros tipos de abuso digital. Estas medias están diseñadas para proteger a los usuarios de comportamientos perjudiciales y garantizar un ambiente en línea más seguro y respetuoso.

En canto a la transparencia en las prácticas de recolección de datos, se espera que las plataformas sean transparentes sobre como recopilan y hacen uso de los datos de los usuarios, incluyendo que los usuarios estén plenamente informados sobre las prácticas de

recopilación de datos, donde se les brinde opciones de control sobre su información personal y proteger su privacidad. Desde el DSA, se reconoce la importancia de la libertad de expresión en línea y busca equilibrarla con la necesidad de mantener los entornos digitales seguros y libres de contenido dañino, también busca proteger la expresión libre y legítima mientras se combate la desinformación y el abuso en línea. Buscando reconocer la importancia de la libertad de expresión en línea y busca equilibrarla con la necesidad de mantener entornos digitales seguros y libres de contenido dañino, queriendo proteger la expresión libre y legítima mientras se combate la desinformación y el abuso en línea.

Por otra parte, el DSA cuenta con la evolución tecnológica y la aparición de nuevas plataformas y servicios digitales, estando diseñado para adaptarse a los avances tecnológicos y a los cambios en el panorama digital, garantizando la relevancia y eficacia de las regulaciones creando así un entorno digital equitativo que fomente la competencia y la innovación. Al establecer reglas claras y transparentes para las plataformas, se pretende crear un campo de juego nivelado que permita que empresas de todos los tambos compitan en igualdad de condiciones y estimulen la creatividad y la diversidad en el sector digital.

Para finalizar, se debe destacar que este reglamento está orientado a fortalecer los derechos de los usuarios en entornos digitales, garantizando la protección de sus datos personales, seguridad en línea y la transparencia en las interacciones digitales buscando empoderar a los usuarios y garantizar que puedan disfrutar de un entorno en línea seguro y beneficioso.

En canto a las sanciones, el reglamento de servicios informáticos establece que en caso de incumplimiento del Reglamento se impondrá una sanción que podrá alcanzar hasta el seis por ciento del volumen de negocio anual, mientras que si la sanción es hace referencia al proporcionamiento de información incorrecta, incompleta o engañosa, o por no someterse a inspección, esta será del uno por ciento del volumen de negocios anual. Y si por un casual se trata de llevar a cabo coacción la multa será del cinco por ciento del promedio diario del volumen de negocio.

**Ley de Mercados Digitales (DMA)**

La Ley de Mercados Digitales, también conocida como Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 es una legislación de la Unión Europea que tiene como objetivo regular a las plataformas digitales y proteger a los usuarios en línea, por ello que se analizarán los puntos más importantes de esta.

La DMA establece que los guardianes de acceso deben de dividirse en tres: el primero son aquellos que se clasifican por su tamaño económico significativo, los cuales son empresa con la capitalización de mercado de al menos setenta y cinco mil millones de euros o volumen de negocios anual en la Unión europea de al menos de 7,5 mil millones de euros. El segundo criterio es el de múltiples servicios interconectados, donde se hace referencia a las empresas que operan al menos en tres estados miembros de la Unión europea y tienen un número significativo de usuarios en múltiples servicios básicos de plataforma como las redes sociales, o los motores de búsqueda. En último lugar se encuentran los que se identifican según su rol central en la cadena de distribución digital donde se encuentran las empresas que actúan como intermediarios entre un gran número de usuarios comerciales y consumidores, haciendo difícil para los usuarios comerciales escapar de su control.

En cuanto a las obligaciones que presentan los “gatekeepers”, encontramos tres vitales, la primera es la obligación de neutralidad de las plataformas donde los guardianes deben velar por la igualdad en el tratamiento garantizando que no se favorezca a sus propios producto y servicios sobre los terceros en términos de acceso y visibilidad en sus plataformas como los resultados de búsqueda, las clasificaciones y recomendaciones. En este punto, también es importante la información sobre modificadores algorítmicos teniendo que informar de manera transparente sobre los principales cambios en los algoritmos que afectan la visibilidad y la ordenación de productos servicios.

En segundo lugar, está la obligación de portabilidad de datos en donde presentan el acceso directo y transferencia segura teniendo que proveer a los usuarios finales y empresariales con herramientas fáciles de usar que permitan exportar y transferir datos a otras plataformas sin obstáculos técnicos o financieros. Así como la compatibilidad de formatos de datos asegurándose que los datos se transfieran en formatos legibles y estandarizados que faciliten la interoperabilidad. Por su parte, la interoperabilidad tiene dos subtareas la primera sería la conocida API abierta y documentadas que facilitan el acceso a interfaces de programación de aplicaciones (API) y servicios de interoperabilidad para terceros desarrolladores, permitiendo que sus servicios se integren efectivamente con la plataforma del guardián. Tambien, se debe tener en cuenta la compatibilidad de sistemas para asegurarse de que los elementos críticos del sistema (como los protocolos de mensajería) sean interoperables con los servicios de terceros.

El siguiente punto para destacar son las prohibiciones para los guardianes como lo es la auto preferencia en donde se indica que queda prohibida la manipulación y la visibilidad de productos y servicios propios de detrimento de los de la competencia

imponiendo condiciones comerciales justas y no discriminatorias para todos los usuarios empresariales que utilizan la plataforma así como bloquear el acceso a los datos generados por empresas terceras quedando prohibido el uso exclusivo de datos generados por usuarios empresariales para fines competitivos propios sin consentir el acceso de las empresas que contribuyeron a su generación. La restricción de la vinculación de servicios imponiendo que queda vetada la atadura contractual determinando que no se puede imponer condiciones que obliguen a la personas o usuarios a usar otros servicios del guardián para acceder a sus servicios principales ayudando a la claridad y transparencia en los términos de los servicios evitando la vinculación oculta o las ventas forzadas.

En cuanto los mecanismos de supervisión encontramos a la comisión europea la cual se encarga de investigar el mercado llevando a cabo investigaciones de mercado, solicitar información, realizando auditorias y entrevistas a las empresas para garantizar el cumplimiento de la DMA determinando sanciones tanto por incumplimiento como por multas coercitivas, en el primer caso la multa alcanza hasta el diez por ciento de su volumen de negocio total a nivel mundial no obstante la comisión podrá imponer al guardián que incumpla una sanción de hasta el 20% de su volumen de negocio, por su parte las multas por negligencia no podrá exceder el 1 por ciento del volumen de negocio. En el caso de las multas coercitivas no podrán exceder el cinco por ciento del volumen de negocio.

En cuanto a las revisiones, estas tendrán carácter periódico donde se revisará la participación de actores del mercado, así como sus procedimientos de consulta para recoger opiniones y feedback (retroalimentación) de los consumidores, competidores y otros actores del mercado sobre la efectividad y a la aplicación del DMA. También se realizarán evaluaciones periódicas cada tres años, de las obligaciones y prohibiciones impuestas a los guardianes, ajustándolas a los rápidos cambios tecnológicos y de mercado.

En el ámbito de la promoción de la innovación y la competencia encontramos la eliminación de e barreras en la que se aplican medidas concretas para la reducción de las barreras de acceso al mercado para nuevas empresas y startups, facilitándoles competir en igualdad de condiciones. También se deberá asegurar que las pequeñas y medianas empresas (PYMEs) tengan acceso equitativo a los datos y recursos necesarios para innovar y crecer. Para finalizar es importante destacar la protección contra las practicas depredadoras donde se supervisa y regulan en las prácticas como la fijación de precios predatorios y cláusulas contractuales abusivas que puedan sofocar la competencia creando incentivos y programas de apoyo para fomentar la innovación en el ecosistema digital.

**Ley de Propiedad Intelectual**

La ley de propiedad intelectual también conocida como Real Decreto Legislativo 1/1996, de 12 de abril abarca una amplia variedad de aspectos legales relacionados con la protección de las creaciones del intelecto humano. Los principales puntos incluyen derechos de autor.

En primer lugar, se habla sobre la protección de las obras generadas por IA donde esta ley aborda la cuestión de la autoría y propiedad de obras generadas por inteligencia artificial, estableciendo si estas obras pueden ser protegidas por derechos de autor y quién sería considerado como autor de estas.

En segundo lugar, la utilización de propiedad intelectual en el Metaverso se hace presente en la normativa puede contemplar la aplicación de derechos de propiedad intelectual en entornos virtuales como el Metaveso, definiendo cómo se pueden proteger y gestionar los derechos de autor, marcas u otros activos intelectuales en este contexto.

En tercer lugar, los contratos inteligentes y propiedad intelectual la ley puede abordar cuestiones relacionadas con la ejecución y validez de contratos inteligentes en el ámbito de la propiedad intelectual, definiendo cómo su pueden gestionar los acuerdos sobre derechos de autor, licencias y otros aspectos relevantes de la propiedad intelectual de forma automatizada y segura.

**Ley de patentes**

La ley de patentes o ley 24/2015 regula la protección de invenciones y la concesión de patentes. En el contexto de la inteligencia artificial la patentabilidad de las invenciones relacionadas con la AI se definen los requisitos y criterios para la concesión de patentes en este campo, como algoritmos de IA o sistemas de aprendizaje automático. En el caso del Metaverso la normativa aborda como se pueden aplicar y hacer valor las patentes en entornos virtuales como el Metaverso, considerando la protección de invenciones relacionadas con tecnologías emergentes en este espacio. En último lugar, los contratos inteligentes la ley regula la cesión y licenciamiento de patentes relacionadas con tecnologías de IA, estableciendo normas para la negociación y ejecución de contratos de licencia en este ámbito

**Ley de Secretos Empresariales**

Ley de Secretos Empresariales o Ley 1/2019, tiene como objetivo fundamental proteger la información confidencial que sea de valor para las empresas y esté sujeta a

medidas de secreto. Esta ley establece disposiciones para la prevención, protección y sanción del uso indebido de secretos empresariales, así como para la defensa de los mismo en caso de infracciones.

Es por esto por lo que la ley puede ser aplicada para la protección de los algoritmos de inteligencia artificial y otros activos intelectuales relacionados con tecnologías de IA como secretos empresariales, otorgado a las empresas herramientas legales necesarias para mantener la confidencialidad y evitar su divulgación no autorizada. También se encarga de garantizar la seguridad y protección de la información confidencial de las empresas en los entornos digitales como el Metaverso. Por último, la normativa otorga relevancia en la negociación y ejecución de los contratos inteligentes que involucran la información confidencial o los secretos empresariales, definiendo las responsabilidades y mecanismos de protección necesarios para preservar la confidencialidad de dichos secretos en un entorno automatizado.

**Directiva sobre Comercio Electrónico**

La Directiva sobre Comercio Electrónico (2000/31/EC) abarca un conjunto de disposiciones detalladas que regulan el comercio en línea en el mercado único digital de la Unión Europea estableciendo pilares fundamentales. En primer lugar, se encuentra la libertad de establecimiento y prestación de servicios, que permite a los proveedores de servicios de la sociedad de la información establecerse y ofrecer servicios en cualquier Estado miembro de la UE sin cumplir requisitos adicionales en cada Estado. Este enfoque fomenta la competencia y amplía el acceso a un mercado más extenso para las empresas en línea. En este sentido, la directiva también establece un marco de responsabilidad limitada para los intermediarios en línea, como los proveedores de alojamiento web, permitiéndoles no ser responsables por la información transmitida o almacenada para sus usuarios en determinadas condiciones, facilitando así la circulación de información en línea.

El siguiente elemento crucial de esta Directiva es la información que los proveedores de servicios de la sociedad deben ofrecer de manera clara y completa a los consumidores antes de que estos finalicen contratos en línea. Esta información incluye detalles sobre la identidad del vendedor, precios totales (con impuestos y gastos de envío), términos y condiciones contractuales, métodos de pago y medidas de seguridad. En cuanto a la publicidad en línea, se establecen normas que exigen claridad, transparencia y veracidad en los mensajes publicitarios, prohibiendo específicamente el envío de publicidad no solicitada por correo electrónico (spam) a menos que se cumplan condiciones

particulares. Asimismo, se promueve la resolución extrajudicial de disputas en línea, brindando a consumidores y comerciantes un mecanismo efectivo para resolver conflictos de forma ágil y accesible, lo que fortalece la confianza en el comercio electrónico y alivia la carga de los sistemas judiciales.

Por último, pero no menos importante, se hace hincapié en la necesidad de garantizar que los consumidores estén debidamente informados al realizar compras en línea. Los proveedores deben suministrar información detallada sobre productos, precios, políticas de devolución, garantías, derechos de desistimiento y otros datos relevantes para facilitar decisiones informadas en el proceso de compra.

**Reglamento eIDAS**

El Reglamento (UE) N.º 910/2014, conocido como eIDAS, se enfoca en regular la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior de la Unión Europea. En este contexto, se profundizará en las aplicaciones particulares de este reglamento en relación con los contratos inteligentes.

Se inicia el análisis con la Identificación Electrónica (eID), donde se establece el marco para el reconocimiento adecuado de los medios electrónicos de identificación entre los países de la UE. En el contexto de los Smart contracts, se requiere que estos contratos inteligentes incorporen un eID para verificar la identidad de las partes involucradas, cumpliendo con los estándares europeos establecidos. Este aspecto se vincula con la función de las firmas electrónicas, las cuales poseen la misma validez legal que las firmas manuscritas y son imprescindibles para la ejecución de los Smart contracts, autenticando a las partes y garantizando la validez legal de los contratos.

En cuanto a los sellos electrónicos, estos se dividen en dos categorías: Sellos electrónicos, que autentican el origen de los datos y aseguran su integridad, y los Sellos de tiempo electrónico, que verifican la fecha de la firma y proporcionan evidencia legal de la hora y fecha de esta. Además, se abordan los servicios de entrega electrónica, los cuales permiten que los Smart contracts faciliten notificaciones y la transmisión segura de datos entre las partes.

Otro aspecto relevante del eIDAS es la implementación de un marco de autenticación para sitios web, con el fin de garantizar la seguridad de las transacciones y prevenir la suplantación de identidad en el contexto de los Smart contracts, asegurando la protección de los usuarios. Por último, se detallan las responsabilidades impuestas a los

proveedores de servicios, quienes deben cumplir con rigurosos requisitos de seguridad y estar sujetos a supervisión periódica para garantizar la confianza en sus servicios.

**Reglamento de Inteligencia Artificial**

El Reglamento de Inteligencia Artificial, o Reglamento COM/2021/206, tiene como propósito primordial mejorar el funcionamiento del mercado interior y propulsar la inserción de la inteligencia artificial enfocada en el ser humano, en concordancia con la salvaguarda de la salud, la seguridad y los derechos fundamentales. En virtud de este objetivo, se definen directrices fundamentales que establece el reglamento, entre las que se hallan disposiciones comunes para la incorporación de sistemas de IA en el mercado de la Unión Europea, restricciones que regirán el ámbito de la IA, requerimientos específicos para sistemas de inteligencia artificial catalogados como de alto riesgo y para sus operadores. A continuación, abordaremos los puntos cruciales que definirán el alcance y el impacto de este reglamento.

El ámbito de aplicación del reglamento se extiende a todos los proveedores que introduzcan o pongan en funcionamiento sistemas de IA en el mercado de la Unión Europea, independientemente de su ubicación dentro o fuera de ésta. Esta medida abarca desde responsables del despliegue, importadores y distribuidores hasta fabricantes de productos que contengan sistemas de IA.

No obstante, se prohíben las actividades vinculadas exclusivamente a la seguridad nacional, defensa o con propósitos militares. Asimismo, quedan exceptuadas las autoridades de terceros países y organizaciones internacionales que hagan uso de sistemas de IA en acuerdos judiciales o con objetivos legales, siempre y cuando proporcionen garantías adecuadas en lo relativo a la protección de los derechos fundamentales. Además, esta normativa complementa, sin afectar negativamente, el marco legal de la Unión en materia de protección de datos personales, privacidad y confidencialidad de las comunicaciones. También quedan excluidos los sistemas IA de código abierto y aquellos dedicados exclusivamente a investigación sin propósitos comerciales.

Prosiguiendo con el análisis del reglamento sobre Inteligencia Artificial, se enfoca en los principios esenciales para el ciclo de vida de los sistemas de IA, subrayando la importancia de la dignidad humana, la transparencia y la responsabilidad. Se delimita la categorización de un sistema de IA de Alto Riesgo y se detallan los requisitos que deben cumplir, asignando a los proveedores la responsabilidad de asegurar la conformidad, lo

cual engloba la implementación de prácticas de gestión de riesgos y datos. Las obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo se orientan a garantizar el cumplimiento de los requisitos; mientras que los importadores y distribuidores se encargan de verificar la conformidad previo a la comercialización. Asimismo, se describen las autoridades responsables de la notificación y los notificados, con procedimientos específicos para la certificación y cumplimiento de sistemas de IA de alto riesgo, incluyendo su registro en la base de datos de la Unión Europea.

El Reglamento prohíbe el uso de técnicas subliminales o manipuladoras en sistemas de IA que puedan influir en las decisiones informadas de las personas y causarles daños. También veta la explotación de vulnerabilidades de individuos por razones de edad, discapacidad o situación social con el fin de modificar su comportamiento negativamente. Se prohíbe valorar o clasificar a personas en base a su comportamiento o características personales si esto conlleva un tratamiento desfavorable, injustificado y desproporcionado. Asimismo, queda prohibida la elaboración de evaluaciones de riesgo de criminalidad basadas únicamente en perfiles personales, a menos que se respalden en valoraciones humanas con hechos verificables. Además, no se permite la creación o ampliación de bases de datos de reconocimiento facial sin criterios selectivos, ni manipular emociones en entornos laborales o educativos, salvo por razones médicas o de seguridad. La clasificación de personas con base en datos biométricos para inferir información sensible como raza, opiniones políticas o creencias religiosas está prohibida, excepto para cumplir con la ley. Por último, el uso de sistemas de identificación biométrica remota (en tiempo real) en espacios públicos solo se permite en circunstancias específicas, como la búsqueda de víctimas de delitos graves o la prevención de amenazas significativas, previa autorización judicial o administrativa y sujeto a una evaluación de impacto en los derechos fundamentales.

Es vital informar a las autoridades de vigilancia y protección de datos sobre la utilización de dichos sistemas, siendo responsabilidad de los Estados miembros establecer normativas detalladas para solicitar, otorgar y supervisar las autorizaciones correspondientes. La Comisión Europea emitirá informes anuales sobre el empleo de sistemas de identificación biométrica remota en espacios públicos, utilizando datos agregados por los Estados miembros.

Dentro del sistema de Gestión de Riesgos para máquinas de inteligencia artificial de alto riesgo, es importante instaurar un proceso continuo de identificación y abordaje de riesgos. Se deben cumplir requisitos específicos para garantizar la conformidad normativa

y la calidad de dichos sistemas. Asimismo, es esencial seguir directrices claras para la gestión de datos de entrenamiento, evaluando posibles sesgos y tomando medidas correctivas para mitigarlos. La presencia de supervisión humana desempeña un papel fundamental para prevenir riesgos para la salud, seguridad y derechos fundamentales durante la utilización de estos sistemas.

En el marco del reglamento, se imponen una serie de responsabilidades a los proveedores de sistemas de inteligencia artificial (IA) de alto riesgo, con la finalidad de asegurar el cumplimiento de los requisitos y normativas establecidas. Esto implica que los proveedores deben garantizar que sus sistemas respeten los estándares especificados, identificando de manera clara la información relevante en el sistema o documentación asociada; implementando un sistema de gestión de calidad para asegurar la calidad y seguridad del producto; mantener documentación específica relacionada con la conformidad; conservando todos los registros generados automáticamente o manualmente por los sistemas; sometiendo periódicamente los sistemas a evaluaciones de conformidad para garantizar que cumplen con los requisitos legales; emitiendo una declaración de conformidad de la Unión Europea para certificar el cumplimiento normativo del sistema de IA; marcando con el distintivo CE que indica la conformidad con las regulaciones de la Unión Europea; cumpliendo con las obligaciones de registro de los sistemas; adoptando y aplicando medidas correctivas cuando sea necesario para asegurar la conformidad; demostrando la conformidad del sistema cuando sea solicitado por la autoridad competente y cumpliendo con otras obligaciones detalladas en el Reglamento.

Respecto a las autoridades notificadoras designadas por cada Estado miembro, se estipula que al menos una autoridad debe ser responsable de supervisar y llevar a cabo los procesos de evaluación, designación y supervisión de los organismos de evaluación. Estas autoridades deben colaborar estrechamente entre sí para facilitar la armonización de los procesos y garantizar un enfoque coordinado en toda la Unión Europea. Es crucial que éstas cuenten con personal competente y especializado en áreas como tecnologías de la información, inteligencia artificial y derecho, para garantizar un enfoque informado y efectivo en la evaluación y supervisión de los sistemas de IA de alto riesgo.

La cooperación entre las autoridades notificadoras de los distintos Estados miembros resulta esencial para asegurar la cohesión y la eficacia en la aplicación de las normas y regulaciones respecto a la IA. Además, se requiere mantener la confidencialidad de la información obtenida durante los procesos de evaluación, respetando la privacidad y protegiendo los datos sensibles de las partes involucradas. La transparencia y la imparcialidad en las actividades de evaluación constituyen pilares clave para garantizar el

cumplimiento normativo y fomentar la confianza en los sistemas de IA de alto riesgo en el mercado europeo.

El artículo 50 del documento establece una serie de obligaciones detalladas para los proveedores y responsables de sistemas de Inteligencia Artificial que impactan directamente a individuos. Este artículo se focaliza en promover la transparencia y divulgar información relevante a los usuarios en relación con la interacción con sistemas de IA. En este sentido, se requiere que los proveedores informen a las personas cuándo interactúan con un sistema de IA, a menos que la naturaleza de la interacción sea obvia para una persona sensata e informada. No obstante, se establecen excepciones para sistemas autorizados que lleven a cabo actividades específicas, como la detección de delitos.

Respecto a los sistemas de IA que generan contenido sintético, se impone el requisito de que los resultados sean claramente identificables como generados artificialmente. De este modo, se establece la responsabilidad de los proveedores de garantizar la eficacia, interoperabilidad y fiabilidad de estas soluciones técnicas, con excepciones como en casos donde la intervención humana es mínima o en actividades autorizadas por ley.

Refiriéndonos al reconocimiento de emociones y la categorización biométrica, se exige a los responsables informar a las personas afectadas sobre el funcionamiento del sistema y el tratamiento de sus datos personales de acuerdo con las regulaciones de la Unión Europea. Por otra parte, en el caso de sistemas que generan o manipulan contenido artificial, se requiere la divulgación de esta circunstancia, a menos que se trate de contenido creativo o de interés público. Esta divulgación debe ser clara y accesible desde el inicio de la interacción.

Es importante subrayar que estas responsabilidades en materia de transparencia no afectan a otras normativas legales establecidas a nivel nacional o de la Unión Europea, y se promueve la creación de códigos de buenas prácticas a nivel de la Unión Europea para garantizar el cumplimiento de estas obligaciones. El propósito fundamental de estas disposiciones es proteger los derechos de los individuos y fomentar una mayor transparencia en la utilización de la IA en la UE.

Se aborda también la clasificación de los "Modelos de IA de Uso General", destacando criterios de clasificación, procedimientos para notificar a la Comisión y obligaciones de los proveedores.

Dentro del reglamento se establecen las "Medidas de Apoyo a la Innovación", resaltando la creación de espacios controlados de pruebas para la IA y las normas para su

establecimiento y operación, el tratamiento de datos personales y las pruebas de sistemas de IA de alto riesgo. Estas medidas buscan fomentar la innovación en la IA, asegurando un entorno controlado para el desarrollo y prueba de sistemas innovadores, así como facilitando el acceso prioritario de pequeñas y medianas empresas a estas oportunidades de prueba y aprendizaje.

A continuación, analizamos exhaustivamente la gobernanza en los sistemas de inteligencia artificial, abarcando la implementación y supervisión de políticas relacionadas con la inteligencia artificial en el contexto de la Unión Europea. Se destaca la creación de la Oficina de IA y el establecimiento del Consejo Europeo de Inteligencia Artificial (Consejo de IA) como entidades fundamentales para consolidar los conocimientos especializados y capacidades en IA a nivel de la Unión. Asimismo, se resalta la importancia de la colaboración entre los Estados miembros para garantizar la coherencia y eficacia en la aplicación del Reglamento.

El Consejo de IA, conformado por representantes de cada Estado miembro, surge como un órgano asesor clave para apoyar tanto a la Comisión como a los Estados miembro en la implementación uniforme del Reglamento. Este Consejo no solo coordina las acciones de las autoridades nacionales competentes, sino que además promueve la armonización de prácticas administrativas y ofrece recomendaciones para mejorar la aplicación efectiva del Reglamento en áreas críticas como la ciberseguridad, la protección de datos y el desarrollo de capacidades digitales.

También se establece un marco consultivo cuyo fin es representar a las partes interesadas a través del Foro Consultivo. La función de este último radica en aportar valiosos conocimientos técnicos para fortalecer las decisiones y acciones del Consejo de IA y la Comisión Europea. Simultáneamente, la constitución de un Grupo de Expertos Científicos Independientes busca proporcionar una perspectiva imparcial y fundamentada en conocimientos especializados, respaldando así la supervisión integral y el cumplimiento efectivo del Reglamento en lo concerniente a la inteligencia artificial de uso general.

A continuación, destacamos la importancia de las autoridades nacionales competentes, que actuarán como pilares fundamentales en la implementación y supervisión del Reglamento, garantizando recursos adecuados y un nivel óptimo de ciberseguridad. Su función proactiva es la asesoría y orientación a las empresas, particularmente a las pymes, reflejando un enfoque integral hacia una ejecución equitativa y eficiente de las disposiciones establecidas en el ámbito de la Unión Europea

Prosiguiendo con el reglamento se alude a la creación y mantenimiento de una base de datos de la Unión Europea para los sistemas de IA de alto riesgo, indicando la

información que debe contener y quiénes son los responsables de introducir los datos. Asimismo, detalla la accesibilidad de la información registrada, la gestión de datos personales y las responsabilidades de la Comisión en el tratamiento de la base de datos.

Por otro lado, se aborda la vigilancia poscomercialización, el intercambio de información y la supervisión del mercado en relación con los sistemas de IA de alto riesgo. Se mencionan los procedimientos de notificación de incidentes graves, la cooperación entre autoridades competentes, la adopción de medidas apropiadas y la importancia de informar a las autoridades correspondientes en caso de incidentes graves.

Además, se introducen disposiciones para garantizar el cumplimiento del reglamento, la supervisión del mercado de sistemas de IA, los poderes de las autoridades encargadas de proteger los derechos fundamentales, las estructuras de apoyo a las pruebas de IA de la Unión, las vías de reclamación y protección de denunciantes, entre otros aspectos trascendentales.

Continuando con el contenido, se subrayan los códigos de conducta y directrices para la aplicación voluntaria de requisitos específicos en sistemas de IA. Se promueve la creación de códigos con gobernanza para sistemas no considerados de alto riesgo, abordando aspectos éticos, sostenibilidad, alfabetización en IA, diseño inclusivo y evaluación de perjuicios para personas vulnerables. La participación en la elaboración incluye a proveedores, responsables de sistemas de IA, organizaciones representativas y partes interesadas, considerando las necesidades de las pymes. Estas directrices de la Comisión Europea detallan la implementación del Reglamento, priorizando las necesidades de las pymes y otros sectores afectados. El Artículo 96 menciona directrices sobre requisitos, prácticas prohibidas, transparencia y relación con actos legislativos de la Unión. Además, el Artículo 97 aborda el ejercicio de la delegación de poderes por parte de la Comisión y el proceso pertinente.

En último término, se detallan las sanciones y multas al instaurar un régimen de sanciones y medidas de ejecución que comprenden multas administrativas de hasta 35.000.000 de euros o hasta el 7% del volumen de negocios total por el incumplimiento de las prácticas de IA. Del mismo modo, se podrán aplicar multas de hasta 15.000.000 de euros o hasta el 3% del volumen de negocios total por el incumplimiento de ciertas obligaciones de operadores y organismos notificados. Además, se podrán aplicar advertencias y medidas no pecuniarias en caso de infracciones de la normativa, así como multas de hasta 7.000.000 de euros o hasta el 1% del volumen de negocios por la provisión inexacta, incompleta o engañosa a organismos notificados o autoridades nacionales.

# 4. CASO PRÁCTICO

La digitalización y la aparición de nuevos activos digitales traen consigo desafíos legales a resolver. En este caso, se analizará la demanda de Nike en contra de StockX para así poder observar cómo afecta la aparición de estos nuevos activos al mercado tradicional.

## Antecedentes

En el caso de la marca de Nike, es una de las empresas de ropa deportiva más importante a nivel global, habiendo sido fundada en el año 1964. Esta presenta fuertes estrategias para la protección de su marca, tomando medidas legales en múltiples ocasiones para proteger sus marcas registradas al igual que sus diseños y sus patentes.

En el otro lado, nos encontramos con StockX, que es una plataforma fundada en el año 2015 y que está especializada en la compra y venta de ropa deportiva. Esta empresa es conocida por sus procesos de verificación de ropa para poder garantizar su autenticidad, abriéndose paso entre los coleccionistas.

Una vez presentadas las dos marcas vinculantes, se pondrá contexto de la demanda. Y es que, con la aparición de los NFTs, la plataforma de StockX decidió lanzar una serie de NFTs para así capitalizar el auge de los nuevos activos digitales. Buscando que los clientes tuvieran una nueva forma de coleccionar, intercambiar y autenticar las zapatillas sin la necesidad de tener el objetivo en físico. Por lo que el sistema funcionaba de la siguiente manera: la plataforma creaba un NFT con el artículo deseado para su posterior venta en la red. Una vez colgado en la red los coleccionistas podrían comprarlo para su posterior canjeo en la tienda o intercambiarlo entre coleccionistas para así poder canjearlo en la tienda por el objeto físico.

## Objeto de la Demanda

- En primera instancia, NIKE demandó a StockX debido a la violación de los derechos de marca registrada y propiedad intelectual debido al lanzamiento de una serie de NFTs por parte de StockX, los cuales estaban inspirados en unas zapatillas físicas incluyendo modelos pertenecientes a NIKE. Por lo que NIKE alegó que se estaba llevando a cabo un uso indebido de su marca afirmando que StockX no tenía autorización para utilizar su propiedad intelectual (como logotipos, nombres de productos y diseños) para la creación de los artículos digitales, manifestando así que los NFTs pese a no ser productos de naturaleza física, podían llegar a generar confusión entre los consumidores, ya que se estaban aprovechando injustamente de la reputación de la marca NIKE.

Por todo lo declarado, NIKE solicitó la prohibición de la comercialización de los NFTS, así como que StockX y sus empresas afiliadas no tengan derecho a hacer uso de los signos-marcas NIKE, teniendo que eliminar los archivos y publicaciones relacionados con los NFTs y que StockX indemnice a NIKE por los daños causados.

Posteriormente, NIKE decidió ampliar la demanda debido a que detectó que algunas zapatillas vendidas en StockX eran de dudosa procedencia, haciendo que NIKE presentará cargos ya que la marca compro zapatillas en StockX resultando ser falsas, lo que conllevo una presentación de pruebas sobre los productos falsificados que supuestamente estaban autenticados por la plataforma StockX. Estos hechos, minaron la credibilidad de la plataforma y disminuyendo la confianza de los consumidores de comprar en los mercados secundarios.

## 4.1 Análisis de la jurisprudencia relevante

Existen varios casos en los que se han visto infringidos los derechos de propiedad intelectual, uno de ellos es el caso de “NIKE vs StockX”, en el cual, aunque no exista una sentencia firme a fecha de hoy, seguro que será un antes y un después para la jurisprudencia relativa a los activos digitales. Es por lo que en el caso NIKE, podemos apreciar las aplicaciones de la jurisprudencia en los siguientes hechos: Infracción de la marca registrada creando así confusión entre los consumidores, utilizando principios como el test Polaroid (creado en el año 1961 y está basado en una serie de puntos en los que el tribunal se fija para así poder evaluar si la marca registrada está siendo infringida), teniendo su fundamento en el caso “Polaroid Corp. contra Polarad Electronics Corp.”

Otro hecho por el que se acusa a StockX es por la supuesta dilución de marca, donde Nike debe demostrar que la venta de los NFTs diluye la distintividad de su marca y si perjudica a su imagen. En donde aparecen los principios de Trademark Dilution Act gracias al caso de “Mosoley contra Secret Ctalogue, Inc.”

Por último, en lo que respecta a los derechos de propiedad intelectual en el contexto digital, existen dos casos que son de interés. El primero es el caso Tiffany (NJ) Inc. contra eBay Inc. en el año 2010 en donde se trataron temas como la venta de productos falsificados. Y el caso de AM General LLC contra Activision Blizzard (2020 ya que se alegaba que se los principios de la propiedad intelectual también deben aplicarse a los NFTs y al contexto digital).

# 5. CONCLUSIONES

Para concluir este trabajo, se ha analizado de una forma exhaustiva los aspectos jurídicos tanto de la inteligencia artificial, como del Metaverso, dejando ver la complejidad existente, así como las intersecciones que se van creando a medida que las regulaciones van avanzando. Es por ello, que las leyes y regulaciones deben de irse abordando a la par que surgen los nuevos desafíos planteados por las Inteligencias Artificiales, el Metaverso y los Smart Contracts, incluyendo sus interacciones conjuntas.

En lo que a las consideraciones futuras observables se trata, estas deben de centrarse en puntos como los derechos individuales, la privacidad de los usuarios, las responsabilidades por parte de cada uno de los participantes en la cadena de uso, la notificación y determinación de los usos indebidos de la tecnología, así como su equidad en el acceso a estas innovaciones tecnológicas.

Por su parte, los desafíos que se presentan frente a estos avances tecnológicos van desde la necesidad de elaborar unos marcos jurídicos claros y actualizados a los momentos actuales, hasta la mitigación de riesgos legales y éticos, así como la creación de unos códigos de conducta. Además de la creación de unas normativas internacionales para regular las tecnologías emergentes, de manera que todos presenten las mismas oportunidades para poder desarrollarse. Es por todo esto, que, en el ámbito de las tecnologías como las IA, y el Metaverso, impere una estrecha relación entre los expertos de estas tecnologías y las autoridades como profesionales del derecho y los responsables políticos para así poder enfrentar estos desafíos de manera eficaz.

## 5.1 Recomendaciones para futuras regulaciones

Para la elaboración de este tipo de investigaciones en el aspecto jurídico de las tecnologías, es recomendable el estudio comparativo de las legislaciones entre las diferentes jurisdicciones, para así poder identificar los puntos débiles de las regulaciones vigentes en ese momento y proponer las soluciones más adecuadas.

Otra de las recomendaciones, sería el de ejecutar un análisis de casos prácticos para ver ejemplos reales y cómo las autoridades y profesionales han sido capaces de desarrollar y resolver los casos, de cara a poder identificar flaquezas en las leyes o cómo se ha aplicado la jurisprudencia en ese ámbito.

Evaluar el impacto tanto legal como ético también es muy importante ya que, si la investigación tratara de temas como la salud, la educación o el comercio electrónico, entre otros, este punto ayudaría a comprender mejor las fortalezas y debilidades que presentan en este caso las tecnologías.

## 5.2 Impacto potencial de futuros desarrollos tecnológicos en la regulación

Los futuros desarrollos tecnológicos presentan la capacidad de repercutir en el campo legal como lo observado con la IA y el Metaverso a lo largo de todo el trabajo. Es por ello, que algunos de los impactos más potenciales son: los cambios en la regulación, ya que habría que readaptar las regulaciones existentes de cara a poder satisfacer la demanda de los nuevos requerimientos. La creación de nuevas áreas legales o regulaciones como ha sido el caso de la ley de Inteligencia Artificial. También se deberá tener en cuenta el cómo afectan las nuevas tecnologías a la privacidad y a la protección de datos para así poder adaptarlas de cara a poder proteger a los usuarios. En último lugar, la responsabilidad y la ética también es un punto importante para tener en cuanta ya que la cadena de actores debe de estar claramente definida de cara a saber quién es el responsable en cada caso.

# 6. REFERENCIAS

Arroyo, R. (2023). Infraestructuras críticas frente a la IA. ciberseguridadTIC. Recuperado el 20 de mayo de 2024, de https://acortar.link/38w12A

ATICO34. (s.f.). Principios de protección de datos (LOPD y RGPD). Grupo ATICO34. Recuperado el 14 de mayo de 2024, de https://acortar.link/XI5yB4

Auditta. (s.f.). Metaverso y protección de datos. Oportunidades y desafíos para las empresas. Auditta. Recuperado el 13 de mayo de 2024, de https://acortar.link/ddm2aU

Ayuso, G. (2022). Derechos de autor y cesión de licencias de uso de NFT. VICOX. Recuperado el 8 de mayo de 2024, de https://acortar.link/JsWfmI

BECK. (2024). Qué es principio de minimización de datos. BECK. Recuperado el 10 de mayo de 2024, de https://acortar.link/zRiFPg

Bench, J. (2023). Guía jurídica de las NFT. HARRIS SLIWOSKI. Recuperado el 10 de mayo de 2024, de https://acortar.link/eZ39GC

BluShark Media. (2023). Propiedad intelectual de NFT: una inmersión profunda en las licencias de marca NFT. Medium. Recuperado el 9 de mayo de 2024, de https://acortar.link/xNLeuU

Cabero Almenara, J., & Puentes Puente, A. (2020). *La Realidad Aumentada: tecnología emergente*. Recuperado el 5 de mayo de 2024, de https://acortar.link/6EuMAf

Casetext. (1961). Polaroid Corp. v. Polarad Electronics Corp. casetext. Recuperado el 25 de mayo de 2024, de https://acortar.link/RrBN5I

COLECCIÓN NFT. (2022). NFTs y Propiedad Intelectual: Todo lo que debes saber. COLECCIÓN NFT. Recuperado el 11 de mayo de 2024, de https://acortar.link/ZRAU94

Comisión Europea. (2021). Paquete de la Ley de Servicios Digitales. Comisión Europea. Recuperado el 17 de mayo de 2024, de https://acortar.link/lRkfBQ

Comisión Europea. (s.f.). *El Reglamento de Servicios Digitales (Digital Services Act - DSA).* Comisión Europea. Recuperado el 16 de mayo de 2024, de https://acortar.link/nnwhNc

Comisión Europea. (s.f.). Reglamento de servicios digitales. Comisión Europea. Recuperado el 17 de mayo de 2024, de https://acortar.link/FIIqSv

Contreras, R. (2023). *Metaverso, qué es, para qué sirve y cómo puede beneficiarnos*. Recuperado el 2 de mayo de 2024, de https://acortar.link/DuxZmV

CRONUTS.DIGITAL. (s.f.). Ejemplos depublicidad en el metaverso. CRONUTS.DIGITAL. Recuperado el 15 de mayo de 2024, de https://acortar.link/3I80WY

del Rosal, P. (2015). Los expertos piden adaptar la ley a las nuevas tecnologías. elEconomista.es. Recuperado el 20 de mayo de 2024, de https://acortar.link/a7YWN0

Díaz Díaz, E. (2022). EVOLUCIÓN DE INTERNET, ¿CUÁLES SON LOS PRINCIPALES RETOS LEGALES DEL METAVERSO?. DERECHO GEOESPACIAL. Recuperado el 21 de mayo de 2024, de https://acortar.link/12isK0

EDPB. (2020). Documento del CEPD sobre el procedimiento para la aprobación de criterios de certificación conducente a una certificación común: el Sello Europeo de Protección de Datos. EDPB. Recuperado el 18 de mayo de 2024, de https://acortar.link/vFJxon

España, G. d. (2023). *Plan de Recuperación, Transformación y resiliencia*. Recuperado el 19 de abril de 2024, de https://acortar.link/S4EMkJ

España, G. d. (2023). Principios. Agencia española protección datos. Recuperado el 9 de mayo de 2024, de https://acortar.link/enSd33

Española, A. (2021). *REALIDAD VIRTUAL REALIDAD AUMNETADA & ABOGACÍA.* Abogacía Española. Recuperado el 4 de mayo de 2024, de https://acortar.link/SqeXt6

Europea, U. (2016). *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.* BOE. Recuperado el 17 de mayo de 2024, de https://acortar.link/P5lBu1

F.fupp., 4. (2020). AM Gen. LLC v. Activision Blizzard, Inc. IPLF. Recuperado el 24 de mayo de 2024, de https://acortar.link/rGGOJz

Gestor RGPD. (2024). Nuevo acuerdo de la Unión Europea sobre inteligencia artificial. Adapta RGPD. Recuperado el 20 de mayo de 2024, de https://acortar.link/mBaX7C

Google. (2024). Usa la privacidad diferencial. Google. Recuperado el 19 de mayo de 2024, de https://acortar.link/CQUDdd

GPO. (2006). TRADEMARK DILUTION REVISION ACT OF. GPO. Recuperado el 23 de mayo de 2024, de https://acortar.link/ehyFMi

Guadamuz, A. (2017). La inteligencia artificial y el derecho de autor. OMPI. Recuperado el 6 de mayo de 2024, de https://acortar.link/K1tNdy

Hao, K. (2021). Caso práctico: probamos por qué un algoritmo judicial justo es imposible. MIT Technology Review. Recuperado el 19 de mayo de 2024, de https://acortar.link/ZVSQ7d

Holdsworth, J. (2023). ¿Qué es el sesgo de la IA?. IBM. Recuperado el 16 de mayo de 2024, de https://acortar.link/yAjDjg

Ibáñez Puente, C. (2022). El Metaverso en el mundo jurídico. ilp ABOGADOS. Recuperado el 21 de mayo de 2024, de https://acortar.link/MxPzjT

Iberdrola. (s.f.). Realidad Virtual: otro mundo al alcance de tus ojos. Iberdrola. Recuperado el 3 de mayo de 2024, de https://acortar.link/y4eVr8

IBM. (2023). ¿Qué es la IA explicable?. IBM. Recuperado el 18 de mayo de 2024, de https://acortar.link/4juuNy

IBM. (2024). *¿Qué es Deep Learning?* Recuperado el 2 de mayo de 2024, de https://acortar.link/tmpftX

INSTITUTO DE INGENIERÍA DEL CONOCIMIENTO. (2024). Inteligencia Artificial responsable: sesgos y explicabilidad. INSTITUTO DE INGENIERÍA DEL CONOCIMIENTO. Recuperado el 16 de mayo de 2024, de https://acortar.link/Xl80fY

Instituto de MERCADOTECNIA Y PUBLICIDAD. (2023). REALIDAD VIRTUAL Y AUMENTADA: SU IMPACTO EN LA PUBLICIDAD. Instituto de MERCADOTECNIA Y PUBLICIDAD. Recuperado el 15 de mayo de 2024, de https://acortar.link/zVTa37

IPLF. (2022). Nike V. Stockx: An Analysis Of The Trademark Infringement In The Metaverse. IPLF. Recuperado el 23 de mayo de 2024, de https://acortar.link/rGGOJz

Iturmendi Morales, G. (2020). Responsabilidad civil por el uso de sistemas de Inteligencia Artificial. laleydigital. Recuperado el 6 de mayo de 2024, de https://acortar.link/vjfeDK

Jefatura del Estado. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE. Recuperado el 18 de mayo de 2024, de https://acortar.link/7fsNk

Labrador Dacal, E. (2023). FASHION LAW: PROTECCIÓN JURÍDICA EN EL METAVERSO. Universidad de Cantabria. Recuperado el 28 de abril de 2024, de https://acortar.link/hFjXIi

LAVOLA. (2017). *ANFAPA*. Recuperado el 30 de mayo de 2024, de https://n9.cl/thc9i1

Legal Skills Prof. (2019). Using Virtual Reality technology to train new courtroom lawyers. LAW PROFESSOR BLOGS NETWORK. Recuperado el 5 de mayo de 2024, de https://acortar.link/z89u4d

mailchimp. (s.f.). Cómo la realidad aumentada está remodelando el panorama del marketing. mailchimp. Recuperado el mayo de 15 de 2024, de https://acortar.link/keTcOv

MELT GROUP. (2023). Sesgos De La IA: ¿Cuáles Son Y Qué Consecuencias Tienen?. MELT GROUP. Recuperado el 16 de mayo de 2024, de https://acortar.link/P6ZRtJ

Ministerio de Asuntos Económicos y Transformación Digital. (2020). Estrategia nacional de INTELIGENCIA ARTIFICIAL. Gobierno de España. Recuperado el 18 de mayo de 2024, de https://acortar.link/gBb2Sr

MINISTERIO DE LA PRESIDIENCIA DE JUSTIACIA Y RELACIONES CON LAS CORTES. (2000). Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre e. GOBIERNO DE ESPAÑA. Recuperado el 22 de mayo de 2024, de https://acortar.link/Dcjxf0

Morell, J. (2021). Cómo la realidad virtual se está usando en el sector legal. Abogacía Española. Recuperado el 3 de mayo de 2024, de https://acortar.link/nU9ykQ

Mutualidad. (2020). El proyecto Legal Speech VR, galardonado con el primer premio del Lab Emprendimiento Jurídico, dotado con 10.000€. Mutualidad. Recuperado el 5 de mayo de 2024, de https://acortar.link/8P4yOA

Nisa Ávila, J. A. (2021). El Metaverso: conceptualización jurídica, retos legales y deficiencias normativas. LEFEBVRE. Recuperado el 8 de mayo de 2024, de https://acortar.link/t5dneH

*OEPM*. (s.f.). Recuperado el 13 de mayo de 2024, de https://acortar.link/N5CFB1

Olavarría, R. (2023). El Metaverso: la adaptación de las marcas y el consumo. upf. Recuperado el 13 de mayo de 2024, de https://acortar.link/tsS1wU

OMPI. (s.f.). *OMPI*. Recuperado el 21 de mayo de 2024, de https://acortar.link/ik9Qqd

Paniagua, E. (2023). Cinco retos de la ley de IA. elespañol. Recuperado el 21 de mayo de 2024, de https://acortar.link/9pYvVS

Park, K. (2022). Marcas en el Metaverso. OMPI. Recuperado el 13 de mayo de 2024, de https://acortar.link/u4LY1s

Parlamento Europeo. (2020). ¿Qué es la inteligencia artificial y cómo se usa? Parlametno Europeo. Recuperado el 18 de mayo de 2024, de https://acortar.link/9D1AgS

Parlamento Europeo. (2024). Reglamento de Inteligencia Artifical. Recuperado el 23 de junio de 2024, de https://acortar.link/tnmJ0E

Parlamento Europeo, C. d. (2009). Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre e. Directorate-General for Communications Networks. Recuperado el 22 de mayo de 2024, de https://acortar.link/suoRYN

Parlamento Europeo, C. d. (2014). Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiv. EUR-Lex. Recuperado el 22 de mayo de 2024, de https://acortar.link/vAqXcL

Parlamento Europeo, C. d. (2014). REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. BOE. Recuperado el 22 de mayo de 2024, de https://acortar.link/akKvH3

Pastor, J. (2016). Privacidad diferencial: Apple presume de ella, Microsoft la creó y Google la usa. Xataka. Recuperado el 19 de mayo de 2024, de https://acortar.link/wLKeyL

Pérez, E. (2022). NFTs y copyright: por qué por mucho dinero invertido los derechos siguen en manos del creador original. Xataka. Recuperado el 12 de mayo de 2024, de https://acortar.link/ZbfQnc

Peritaciones MGA. (2014). ¿Ecommerce o Wild Wild West? Tiffany vs eBay. Peritcaciones MGA. Recuperado el 24 de mayo de 2024, de https://www.peritacionesmga.com/blog/es/tag/tiffany-vs-ebay/

Pombo Nartallo, V. (2023). ¿Qué es la explicabilidad de la inteligencia artificial? Cómo quitarle misterio a la tecnología. BBVA. Recuperado el 19 de mayo de 2024, de https://acortar.link/cj8S0O

Rebold Marketing. (2022). Realidad virtual y realidad aumentada: cómo están cambiando las reglas del marketing digital. Rebold Marketing. Recuperado el 15 de mayo de 2024, de https://acortar.link/BKgLFQ

Sáez Hurtado, J. (2022). Qué es el metaverso, ejemplos y cómo se accede. IEBS. Recuperado el 30 de abril de 2024, de https://acortar.link/lj3mQG

Sanchis, A. (2024). Incendio en Google: tiene un problema con su IA (y su futuro), y le está costando millones. El Confidencial. Recuperado el 16 de mayo de 2024, de https://acortar.link/C6jQcU

Sanofi. (2023). Usos de la inteligencia artificial en medicina y sus beneficios en la salud de los pacientes. Sanofi. Recuperado el 3 de mayo de 2024, de https://acortar.link/BJuRSk

SAP. (s.f.). ¿Qué es la realidad aumentada (AR)? SAP. Recuperado el 2 de mayo de 2024, de https://acortar.link/UlfuXY

Schrepel, T. (2021). Los contratos inteligentes y el mercado único digital a través de un enfoque de «legislación más tecnología». Comisión Europea. Recuperado el 21 de mayo de 2024, de https://acortar.link/7Fk1Ra

SECOND LIFE. (2011). Linden Lab Official:Technical overview of Second Life security. SECOND LIFE. Recuperado el 19 de mayo de 2024, de https://acortar.link/cIRoKs

Segura Venegas, C. Á. (2019). Jurisprudencia Española y Estadounidense acerca de la Protección Jurídica de los Videojuegos y su Originalidad. UNIVERDIAD INTERNACIONAL DE LA RIOJA. Recuperado el 25 de mayo de 2024, de https://acortar.link/nwxTZP

servicenow. (s.f.). ¿Qué es una licencia perpetua? servicenow. Recuperado el 10 de mayo de 2024, de https://acortar.link/hgv8Rr

squarepoint. (2024). ¿Cómo afecta la nueva Ley de Inteligencia Artificial a la Gestión de Personas?. squarepoint. Recuperado el 20 de mayo de 2024, de https://acortar.link/vW9voI

UEIPO. (2024). *UEIPO*. Recuperado el 25 de mayo de 2024, de https://www.euipo.europa.eu/es

Veale, M. y. (2021). Demystifying the Draft EU Artificial Intelligence Act. Degruyter. Recuperado el 15 de mayo de 2024, de https://doi.org/10.9785/cri-2021-220402

Veltani, J. D., & Mansilla, M. B. (2023). Avatares y propiedad intelectual. AVOA abogados. Recuperado el 30 de abril de 2024, de https://acortar.link/4ECcxS

Wattanajantra, A. (2024). Ley de IA de la Unión Europea: ¿Qué significan las leyes de inteligencia artificial para las empresas?. Sage. Recuperado el 20 de mayo de 2024, de https://acortar.link/vW9voI

Zorraquino, A., & Martí Casado, J. (2022). Primera resolución judicial en España sobre los NFTs: reproducción y transformación. PwC. Recuperado el 13 de mayo de 2024, de https://acortar.link/XPIHTv