



**Universidad del Azuay**

**Facultad de Ciencias Jurídicas**

Escuela de Derecho

**HACIA LA REGULACIÓN Y CONTROL DE  
LA INTELIGENCIA ARTIFICIAL: LA  
TUTELA AL DERECHO DE PROTECCIÓN DE  
DATOS**

Autora:

**María Emilia Reyes Toral**

Director:

**Guillermo Alejandro Ochoa Rodríguez, PhD.**

**Cuenca – Ecuador**

**2024**

**DEDICATORIA**

A mis padres, Juan Carlos y María Fernanda, a mi hermana Mercedes, por su amor y apoyo incondicional.

A Chester, por estar a mi lado siempre.

## **AGRADECIMIENTOS**

A mi profesor Guillermo Ochoa Rodríguez, por su valiosa orientación y dedicación en todo este proceso.

A mis compañeros y amigos, por su apoyo constante, motivación y por compartir este camino conmigo.

A mi familia, especialmente a mis abuelos, Jaime, Fanny, Arturo y Catalina, por su amor incondicional, sus enseñanzas y por ser mi fuente de fortaleza.

## RESUMEN

Este trabajo de titulación examina inicialmente la evolución histórica de la Inteligencia Artificial (IA) y su relación con el derecho. Se analiza cómo el rápido avance de la IA, ha incurrido en la falta de una regulación adecuada, lo que ha permitido la vulneración de derechos fundamentales, primordialmente el derecho a la protección de datos personales. El enfoque principal es un análisis de las regulaciones normativas existentes, iniciando por el marco normativo ecuatoriano, seguido de un análisis comparativo con regulaciones internacionales, lo que permite identificar las diferencias en la regulación de la IA entre diversos países. También se exploran las implicaciones éticas derivadas del uso autónomo de esta tecnología en la recopilación de datos. Se presentan ejemplos de casos que evidencian la vulneración del derecho a la protección de datos para ilustrar la magnitud del desafío actual.

Finalmente, se proponen recomendaciones basadas en el análisis de las normativas estudiadas, sugiriendo mejoras a los reglamentos existentes y aportando ideas para aquellos países que aún carecen de regulaciones específicas. La investigación revela que, aunque existen esfuerzos normativos en varios territorios, muchos de ellos resultan insuficientes. La regulación más avanzada identificada es la de la Unión Europea, la cual se recomienda como modelo para otros países. La metodología empleada fue cualitativa, con un enfoque descriptivo y bibliográfico, centrado en el análisis jurídico de diversas normas internacionales.

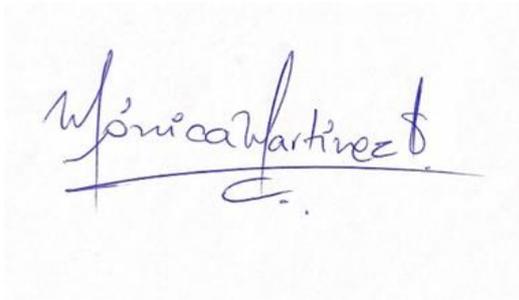
**Palabras clave:** derecho comparado, derecho de protección de datos personales, ética digital, inteligencia artificial, privacidad.

## ABSTRACT

This thesis explores the evolution of Artificial Intelligence (AI) and its interplay with the legal framework, focusing on how insufficient regulation has led to violations of fundamental rights, particularly personal data protection. It begins with an examination of the Ecuadorian regulatory framework, followed by a comparative analysis of international standards to highlight regulatory disparities across countries. Additionally, the ethical challenges posed by autonomous AI systems in data collection are analyzed, underlining their impact on privacy and trust. Case studies illustrate real-world instances of data protection violations, underscoring the urgency for robust regulation. Based on this analysis, the study offers recommendations to enhance existing regulations and guide nations lacking AI-specific frameworks. The European Union's advanced regulatory approach is identified as a model for other countries. The research employs a qualitative methodology with a descriptive and bibliographic approach, centered on legal analyses of international norms.

**Keywords:** comparative law, personal data protection law, digital ethics, artificial intelligence, privacy.

Approved by

A handwritten signature in blue ink, reading "Mónica Martínez Sojos" with a horizontal line underneath.

Lcda. Mónica Martínez Sojos, Mgt.

Cod.29598

## ÍNDICE DE CONTENIDO

Dedicatoria .....	ii
Agradecimientos .....	iii
Resumen .....	iv
Abstract .....	v
Índice de Contenido .....	vi
Índice de Tablas .....	vii
Introducción .....	1
1. Inteligencia Artificial y Derecho: Fundamentos y Protección de Datos .....	3
1.1. Concepto y Orígenes de Inteligencia Artificial (IA).....	3
1.2. Inteligencia artificial y su vinculación con el derecho.....	4
1.3. Relación entre la Inteligencia Artificial y la Protección de Datos Personales. ....	6
1.4. Tratamiento del derecho a la protección de datos personales en nuestro derecho interno .....	8
2. Estándares Internacionales en la Regulación de la IA y la Protección de Datos. ....	12
2.1. Comparativa de Regímenes Regulatorios Internacionales.....	12
2.2 Implicaciones Éticas sobre el uso de la IA, en la recopilación, procesamiento y uso de datos personales.....	18
2.3 Estudio de Casos sobre la vulneración del derecho de protección de datos personales por sistemas de IA.....	19
3. Propuestas y recomendaciones a reglamentos previamente analizados .....	24
3.1 Ecuador .....	24
3.2 Estados Unidos .....	27
3.3 China.....	29
3.4 Unión Europea .....	30
Conclusiones .....	33
Referencias .....	35

**ÍNDICE DE TABLAS**

<b>Tabla 1</b> <i>Normativa AI Act</i> .....	15
--	----

# INTRODUCCIÓN

Hoy en día, la inteligencia artificial se ha convertido en un tema recurrente en nuestras conversaciones cotidianas. Esta tecnología ha logrado integrarse profundamente en muchos aspectos de nuestras vidas, cambiando la forma en que trabajamos, nos comunicamos y accedemos a la información. No obstante, su impacto no ha sido exclusivamente positivo. Si bien ha facilitado procesos y creado oportunidades antes inimaginables, también ha generado efectos negativos que afectan a la sociedad de diversas maneras. A pesar de estar al alcance de todos, la falta de un control adecuado ha permitido que cause daños significativos. Uno de los problemas más preocupantes es la vulneración de derechos fundamentales, como el derecho a la protección de datos personales. Es por ello que resulta imperativo realizar un análisis profundo sobre cómo la inteligencia artificial ha comprometido este derecho esencial.

Este trabajo de titulación se enfoca en evaluar la urgencia de tomar medidas concretas para regular estos sistemas, que, si bien fueron diseñados para hacer nuestras vidas más sencillas, presentan desafíos importantes que no deben ser ignorados. Como toda innovación tecnológica, la inteligencia artificial trae consigo tanto ventajas como desventajas, y es nuestra responsabilidad establecer los límites necesarios para que su desarrollo no comprometa nuestros derechos ni nuestra seguridad.

En este sentido, la regulación de la inteligencia artificial se presenta como un desafío complejo pero ineludible. La rapidez con la que estas tecnologías avanzan ha dejado atrás a los marcos legales existentes, que no logran adaptarse a la velocidad ni a la magnitud de los cambios que generan. La falta de normativa específica ha permitido que los sistemas de inteligencia artificial operen en zonas grises, donde los derechos individuales, como la privacidad y la protección de datos personales, se ven comprometidos sin que existan mecanismos claros para prevenir o sancionar estos abusos. Este vacío legal no solo pone en riesgo la información personal de las personas, sino que también abre la puerta a la explotación y manipulación de datos a gran escala.

Por ello, es esencial que se implementen regulaciones que no solo controlen el uso de la inteligencia artificial, sino que también protejan los derechos de los individuos en esta nueva era digital. Este trabajo busca, entonces, no solo analizar las vulneraciones que ya han ocurrido y analizar la normativa existente, sino proponer soluciones concretas que nos permitan avanzar hacia un uso más ético y responsable de la inteligencia artificial,

garantizando que esta poderosa herramienta sirva para el bienestar colectivo y no se convierta en una amenaza a nuestras libertades fundamentales.

# CAPÍTULO 1

## 1. INTELIGENCIA ARTIFICIAL Y DERECHO: FUNDAMENTOS Y PROTECCIÓN DE DATOS

### 1.1. Concepto y Orígenes de Inteligencia Artificial (IA)

Desde una perspectiva técnica, el término "inteligencia artificial" (IA) se emplea habitualmente para describir la capacidad de una máquina de replicar las funciones cognitivas propias de los seres humanos, como el razonamiento, la toma de decisiones y el aprendizaje. No obstante, este concepto ha evolucionado y se ha diversificado a lo largo del tiempo, dando lugar a nuevas áreas de estudio y desarrollo dentro del campo de la IA. Una de estas áreas emergentes es el aprendizaje automático, o "machine learning", donde los sistemas son diseñados para aprender de manera autónoma a partir de datos, ejemplos y experiencias. En este enfoque, las máquinas no solo ejecutan tareas preprogramadas, sino que también mejoran su rendimiento y precisión a medida que procesan más información y adquieren conocimientos sobre los patrones y comportamientos de los usuarios que interactúan con ellas (Enríquez, 2021).

A lo largo de la historia, la humanidad ha mostrado un interés constante por replicar comportamientos inteligentes. Desde la antigüedad, como lo demuestran juegos matemáticos como las Torres de Hanói, que se remontan al 3000 a.C., se ha explorado cómo alcanzar metas utilizando la menor cantidad de acciones posibles, un principio fundamental en la inteligencia artificial (IA). Esta idea no es nueva; ya en el 322 a.C., Aristóteles imaginaba la posibilidad de crear máquinas que pudieran razonar (IEEE & Ministerio de Defensa, 2017).

A través de los siglos, este interés ha dejado su marca en diferentes avances históricos, impulsando el desarrollo de tecnologías que emulen la inteligencia humana. Hoy en día, la IA es una realidad, fruto de siglos de reflexión y experimentación sobre cómo dotar a las máquinas de capacidades cognitivas. Este recorrido resalta la profunda relación entre la búsqueda del conocimiento y la innovación tecnológica, que ha llevado a la creación de sistemas inteligentes cada vez más avanzados.

Otro avance significativo dentro de la inteligencia artificial es el desarrollo de modelos de redes neuronales. Estos modelos se inspiran en la estructura y el

funcionamiento del cerebro humano, con el objetivo de mejorar la capacidad de procesamiento y toma de decisiones de las máquinas. Las redes neuronales permiten a los sistemas de IA abordar problemas complejos, como el reconocimiento de imágenes y el procesamiento del lenguaje natural, de una manera más eficiente y precisa (Enríquez, 2021).

Asimismo, la inteligencia artificial se encuentra íntimamente relacionada con los metadatos, lo que hace imprescindible su definición y comprensión. En términos simples, los metadatos son datos que proporcionan información sobre otros datos. En otras palabras, son "datos sobre datos". Su función principal es describir, organizar y facilitar el acceso a la información contenida en un archivo o un objeto digital; Estos actúan como una estructura subyacente que define y organiza los datos, permitiendo que estos objetos interactúen y se integren en redes más amplias. Por lo que los objetos digitales adquieren sentido no solo por su contenido, sino por las relaciones que los metadatos establecen con otros objetos dentro de un sistema digital más complejo (Hui, 2017).

En este sentido, los metadatos trascienden su función de simples descripciones, convirtiéndose en elementos esenciales que configuran la "realidad digital" y permiten el adecuado funcionamiento de la web y las aplicaciones tecnológicas. Actúan como un puente fundamental que conecta las interacciones humanas con las tecnológicas, facilitando la comunicación y el intercambio en un ecosistema digital en constante evolución (Hui, 2017).

A medida que estas tecnologías continúan avanzando, el alcance y la definición del término "inteligencia artificial" seguirán expandiéndose. Nuevas aplicaciones y retos surgirán con el tiempo, reflejando la constante evolución tecnológica en este campo. Por lo tanto, el concepto de IA no solo abarca la imitación de las capacidades humanas por parte de las máquinas, sino que también se está convirtiendo en un término paraguas que incluye diversas disciplinas y enfoques, cada uno con su propia importancia y potencial en el futuro de la tecnología. (Enríquez, 2021).

## **1.2. Inteligencia artificial y su vinculación con el derecho**

El rápido avance de la inteligencia artificial (IA) está permeando casi todos los aspectos de nuestra vida diaria, desde campos especializados como la ingeniería aeroespacial y la robótica hasta tareas cotidianas como escuchar música o utilizar un

celular. Este progreso está generando tanto incertidumbres como riesgos, y está poniendo a prueba las normativas legales existentes, ya que la creación de una inteligencia no biológica capaz de superar las capacidades cognitivas humanas está dando lugar a nuevas relaciones jurídicas que no habían sido contempladas anteriormente.

En el campo del derecho, la interacción con la inteligencia artificial (IA) se manifiesta en dos vertientes principales. Por un lado, el derecho regula el uso y desarrollo de la IA, estableciendo marcos legales y normativos que buscan controlar los riesgos asociados con su implementación, asegurando que su desarrollo y aplicación no vulneren derechos. Este enfoque es esencial en un mundo donde la IA tiene un impacto creciente en diversos aspectos de la vida cotidiana y plantea desafíos éticos y jurídicos que requieren una respuesta legal. Por otro lado, la IA se aplica dentro del ámbito jurídico, mejorando procesos como la investigación legal, la toma de decisiones judiciales y la administración de justicia. Sin embargo, es en la primera rama donde el derecho juega un papel crucial como guardián, estableciendo límites, responsabilidades y salvaguardas para garantizar que el avance de la IA se realice de manera segura (Cáceres Nieto, 2023).

A medida que la IA evoluciona, surgen desafíos filosófico-jurídicos sobre cómo el derecho debe abordar la integración de máquinas con niveles avanzados de autonomía y consciencia. Además, el uso masivo de IA está comenzando a vulnerar derechos fundamentales, como el derecho a la protección de datos personales, lo que añade una capa de complejidad al desafío legal. Hasta ahora, la respuesta del derecho ha sido pragmática, abordando los problemas de manera específica en áreas como el derecho civil, penal o laboral, pero sin desarrollar una teoría general que guíe estas nuevas realidades. Esta aproximación, aunque funcional, está creando una desconexión entre la evolución tecnológica y la normativa, llevando a una obsolescencia que se acentúa con cada nuevo avance en IA (Parra Sepúlveda & Concha Machuca, 2021).

Frente a este desafío, es crucial adoptar una doble estrategia: por un lado, avanzar en la creación de normas sectoriales que respondan a los problemas emergentes de la IA, y por otro, reflexionar desde la teoría del derecho para establecer principios y marcos normativos flexibles que puedan adaptarse al constante cambio tecnológico (Parra Sepúlveda & Concha Machuca, 2021).

### **1.3. Relación entre la Inteligencia Artificial y la Protección de Datos Personales.**

Los sistemas de Inteligencia Artificial (IA) manejan extensas cantidades de datos, muchos de ellos de carácter personal, a menudo sin el conocimiento o consentimiento explícito de los individuos afectados. Estos dispositivos, al integrarse de forma sutil en la vida cotidiana, recolectan información de manera extensiva, y su capacidad para procesar datos de manera compleja puede generar resultados inesperados a partir de datos que están fragmentados.

Esta situación plantea serias complicaciones para la protección de la privacidad, al tiempo que resalta la urgencia de un seguimiento minucioso de las tecnologías de IA para prevenir abusos. Es esencial investigar cómo estas tecnologías podrían influir en la libertad individual y tener un impacto desproporcionado en grupos vulnerables, como los menores, para desarrollar mecanismos que aseguren una mayor transparencia y responsabilidad en el manejo de datos personales. Además, considerar la integración de principios de derechos humanos en la regulación de la IA podría proporcionar un marco ético que guíe la protección de la privacidad en la era digital, equilibrando la innovación tecnológica con el respeto a los derechos fundamentales (Fernández-Aller & Serrano Pérez, 2022).

Los datos personales son fundamentales para nuestra vida privada y afectan nuestras actividades diarias, ya que son cualquier dato que contenga una característica identificadora de una persona de forma directa o indirecta, al revelar aspectos íntimos como información financiera, relaciones personales, datos de salud, fechas de nacimiento, números de teléfono, etc. Por lo tanto, es crucial garantizar su seguridad y confidencialidad. Este derecho se encuentra protegido por la Constitución de la República del Ecuador, en el artículo 66, núm. 19, otorgando así a los individuos el control sobre su información, permitiéndoles decidir su uso y acceso (Constitución de La República Del Ecuador, 2008).

Para un mayor entendimiento acerca de todo lo que abarcan los datos personales, se realizará una breve clasificación de estos. De acuerdo con León Carvajal (2009), los datos personales pueden dividirse en un alcance público o privado:

- a) Públicos: Estos datos personales son denominados "públicos" porque son accesibles para un amplio número de personas. Su difusión suele estar

relacionada con su presencia en registros oficiales, como el nombre, apellido, dirección, etc., los cuales están disponibles a través de fuentes de acceso público. Sin embargo, si el titular lo desea, puede impedir su difusión.

b) Privados: Se les denomina "privados" porque es el titular de dichos datos quien tiene la facultad de decidir si los comparte con terceros. En determinadas circunstancias, sin embargo, puede estar obligado a proporcionarlos, como en el caso de exigencias legales. Estos datos, a su vez, se subdividen en categorías de "íntimos" y "secretos," dependiendo de su naturaleza y el nivel de confidencialidad que requieren.

a. Datos Íntimos y Secretos: Por un lado, los datos íntimos son aquellos que revelan aspectos esenciales de la personalidad, como creencias, ideologías y pensamientos del individuo. Este tipo de información puede ser protegida, y su difusión no debe llevarse a cabo a menos que exista una obligación legal o una decisión voluntaria de compartirla. Por otro lado, los datos secretos son aquellos que el individuo no está obligado a revelar a ninguna persona, salvo en casos donde decida hacerlo de manera voluntaria (León Carvajal, 2009)

Aunque la legislación actual busca salvaguardar la privacidad y asegurar que los datos sean precisos y utilizados sólo con fines específicos, la rápida expansión y el avance constante de la inteligencia artificial (IA) han creado grandes retos. La falta de una normativa adecuada y actualizada en este ámbito ha llevado a que el derecho a la protección de datos sea frecuentemente vulnerado por estos sistemas avanzados. En consecuencia, proteger la información personal se vuelve aún más crítico en un entorno donde las tecnologías digitales permiten una difusión masiva e ilimitada de datos, generando la necesidad urgente de desarrollar marcos regulatorios que puedan seguir el ritmo de la evolución tecnológica (Arellano López, 2020)

La inteligencia artificial (IA), como se mencionó anteriormente, se sustenta en gran medida en el procesamiento de datos, y aunque no siempre involucra datos personales, la relación entre ambos es innegable. Los datos personales se convierten en un recurso fundamental para el funcionamiento de la IA, y cuando son recolectados a gran escala, se

corre el riesgo de vulnerar el derecho a la protección de esta información. Las empresas que actúan como intermediarias de datos, al emplear herramientas de IA, suelen utilizar datos personales de sus usuarios para tomar decisiones automatizadas que tienen un impacto significativo en sus vidas. Estas decisiones pueden ir desde evaluar la aptitud para obtener un crédito, acceder a información médica sin el consentimiento adecuado, o determinar la idoneidad para un puesto de trabajo, hasta decidir qué publicidad y contenidos se mostrarán a cada usuario. Esta situación pone de relieve la necesidad de que la protección de datos personales sea una prioridad en el desarrollo y aplicación de la IA, garantizando que estos sistemas operen de manera ética y respetuosa con la información de los individuos y a su vez sus derechos sean respetados (Albornoz, 2021).

#### **1.4. Tratamiento del derecho a la protección de datos personales en nuestro derecho interno**

La protección de datos personales se establece como una rama fundamental del derecho, cuyo objetivo primordial es garantizar la libertad individual al preservar la privacidad en el contexto del tratamiento de información, ya sea de manera manual o automatizada. Este campo legislativo no se limita únicamente a salvaguardar el derecho a la intimidad, sino que también abarca la protección de una amplia gama de bienes e intereses que pueden verse vulnerados mediante la recolección y el procesamiento de datos sobre individuos identificables o identificados (Machuca Vivar et al., 2022).

En Ecuador, el reconocimiento constitucional del derecho a la protección de datos personales ha experimentado un desarrollo notable. La reforma constitucional de 1996 incorporó la garantía del habeas data como un mecanismo para salvaguardar la información personal. No obstante, fue en 2008 cuando este derecho adquirió un estatus autónomo y fundamental en la Constitución, inspirado por los elevados estándares europeos en la materia. Esta normativa establece que la recolección, almacenamiento, procesamiento, distribución o divulgación de datos personales debe contar con el consentimiento del titular o estar amparada por una disposición legal específica (Rosas-Lanas & Pila-Cárdenas, 2023).

A pesar de este avance, la Constitución no definió con claridad los alcances ni los mecanismos para ejercer este derecho, lo que llevó a la promulgación de la Ley Orgánica de Protección de Datos Personales en el año 2021. Hasta hace poco, Ecuador era uno de los pocos países latinoamericanos sin una Ley de Protección de Datos Personales, a

diferencia de otras naciones que cuentan con legislaciones similares desde hace dos décadas. La promulgación de esta ley marcó un paso significativo hacia la regulación adecuada del manejo de datos personales, haciendo imperativo que los responsables del tratamiento de información se familiaricen con la normativa para evitar infracciones (Machuca Vivar et al., 2022).

Esta ley estableció los principios fundamentales, derechos y obligaciones, así como los mecanismos de protección en este ámbito. Sin embargo, a medida que las tecnologías de la información, las amenazas cibernéticas y los sistemas de inteligencia artificial se vuelven más sofisticados, persisten los desafíos en el campo de la protección de datos personales, especialmente en un contexto donde otros derechos fundamentales, como la vida, la salud y el trabajo, también pueden verse comprometidos (Rosas-Lanas & Pila-Cárdenas, 2023).

Aunque la Ley Orgánica de Protección de Datos Personales en Ecuador establece un marco legal para el manejo y protección de la información personal, esta no contempla específicamente la regulación de la inteligencia artificial ni prevé sanciones para las infracciones a este derecho cometidas por dichos sistemas. La ausencia de disposiciones específicas sobre la IA en la normativa genera un vacío legal en cuanto a la responsabilidad y manejo de estas tecnologías en casos de violación a la protección de datos. En un escenario donde la inteligencia artificial adquiere un rol cada vez más preponderante en el procesamiento de datos, esta laguna normativa pone en entredicho la efectividad de la ley y la tutela efectiva de los derechos fundamentales de las personas.

La nueva iniciativa legal presentada el 26 de junio del 2024, por la legisladora Patricia Núñez para regular el uso de la Inteligencia Artificial (IA) en Ecuador busca establecer un marco normativo exhaustivo que abarque tanto el impacto presente como futuro de la IA en los derechos fundamentales y en la cohesión social. El proyecto, compuesto por 83 artículos, subraya la importancia de aprovechar el potencial transformador de la IA para impulsar el progreso económico, social y ambiental, así como para optimizar la eficiencia de los servicios públicos y privados (Núñez Ramos, 2024).

Un aspecto crucial del proyecto es su enfoque en la protección de datos personales, abordando específicamente el tratamiento masivo de datos y estableciendo principios y obligaciones para garantizar su uso adecuado (Montenegro, 2024). Se introducen medidas para fortalecer la IA como una herramienta segura y ética, con un énfasis en preservar la

privacidad y asegurar que el tratamiento de datos personales cumpla con altos estándares de protección. Además, el proyecto establece niveles de riesgo para la implementación de sistemas de IA, prohibiendo aquellas aplicaciones que atenten contra la dignidad humana o la seguridad nacional. La legisladora enfatiza la necesidad de adoptar la IA de manera responsable para maximizar sus beneficios y mitigar los riesgos asociados (Nuñez Ramos, 2024).

La asambleísta Karina del Carmen Subia también ha propuesto un proyecto de ley para fomentar y desarrollar la Inteligencia Artificial en Ecuador. Aunque este proyecto incluye de manera parcial consideraciones sobre la protección de datos personales, su enfoque principal se dirige hacia el estímulo del desarrollo del software y la inversión en el sector tecnológico. Este énfasis busca posicionar a Ecuador como un actor relevante en la revolución digital, fomentando la creación de nuevas tecnologías y aplicaciones que impulsen el crecimiento económico (Ponce & Espinosa Velarde, 2024).

A diferencia de la iniciativa presentada por la asambleísta Patricia Núñez, que ofrece un marco normativo detallado para regular la IA y proteger los derechos fundamentales, el proyecto de Subia no aborda con la misma profundidad la salvaguarda de la información personal. Este enfoque más limitado en la protección de datos revela una brecha significativa en la normativa, ya que no proporciona una cobertura exhaustiva para garantizar la privacidad y la seguridad de los datos en el contexto del avance tecnológico.

A pesar de la ausencia de regulaciones internas específicas y detalladas que aborden de manera integral el uso de la Inteligencia Artificial (IA) en el contexto de la protección de datos personales, se han logrado avances significativos en la legislación ecuatoriana. El reconocimiento del derecho a la protección de datos personales como un derecho fundamental en la Constitución de 2008 marcó un hito crucial en la consolidación de la privacidad y la seguridad de la información personal. Este avance se complementó con la promulgación de la Ley Orgánica de Protección de Datos Personales en 2021, que estableció un marco normativo para la gestión y protección de los datos en el país, el cual fue desarrollado en el reglamento a la referida ley, en noviembre de 2023. Sin embargo, a pesar de estos avances, aún no se ha desarrollado una regulación específica que aborde los retos particulares que plantea la IA en términos de protección de datos.

En este contexto, la presentación de proyectos de ley por parte de las asambleístas Patricia Núñez y Karina del Carmen Subia representa un paso importante hacia la creación de una normativa interna más completa y ajustada a las demandas actuales. La iniciativa de Núñez ofrece un marco más completo para la regulación de la IA y la protección de datos personales, abordando de manera más exhaustiva los desafíos emergentes. Por otro lado, el proyecto de Subia, aunque enfocado principalmente en el fomento del desarrollo tecnológico, también apunta a avanzar en la integración de la IA en el país. Estos esfuerzos legislativos subrayan la urgencia de adaptar y fortalecer el marco normativo para enfrentar los nuevos retos en la intersección de la tecnología y la protección de los derechos fundamentales, como lo es el derecho de protección de datos personales.

## **CAPÍTULO 2**

# **2. ESTÁNDARES INTERNACIONALES EN LA REGULACIÓN DE LA IA Y LA PROTECCIÓN DE DATOS.**

### **2.1. Comparativa de Regímenes Regulatorios Internacionales.**

En los últimos años, la Inteligencia Artificial (IA) ha experimentado un crecimiento vertiginoso, impulsando avances tecnológicos a un ritmo sin precedentes. Sin embargo, la rapidez con la que estas tecnologías emergen y se implementan ha superado en muchos casos la capacidad de los sistemas legales para regularlas de manera efectiva. Aunque en la mayoría de los países aún no existen regulaciones exhaustivas que aborden todos los aspectos relacionados con la IA, algunos países han comenzado a desarrollar marcos normativos específicos para gestionar su impacto, algunos en relación con lo que concierne a la protección de datos personales y la ética en su aplicación. A continuación, se analizarán algunos de los avances más importantes.

La regulación de la Inteligencia Artificial (IA) en Estados Unidos ha experimentado un desarrollo complejo, dado que las normativas sobre el tratamiento de datos son inconsistentes entre los diferentes estados, lo que genera variabilidad en los niveles de seguridad y en los requisitos aplicables. No obstante, existen ciertas regulaciones de carácter federal, aprobadas por el Congreso de los Estados Unidos, que tienen aplicación en todo el país. Estas normativas han comenzado a introducir sutiles cambios en el panorama regulatorio de la IA, aunque su impacto sigue siendo limitado en comparación con los desafíos que plantea esta tecnología en evolución.

Comenzando con la National Defence Authorization Act for Fiscal Year 2020. Esta ley, promulgada bajo la presidencia de Donald Trump, abordó principalmente temas generales relacionados a los objetivos y prioridades para la defensa nacional de los Estados Unidos. Sin embargo, aunque muy vagamente, por primera vez se trataron problemas como los riesgos asociados con los deepfakes, las cuales manipulan imágenes y videos basados en inteligencia artificial que permite crear contenido visual falso, pero extremadamente realista, subrayando así la necesidad de una supervisión en torno a la manipulación digital en procesos críticos como las elecciones (Rodríguez Cardona, 2023).

La administración de Joe Biden intentó ampliar el enfoque con la National Artificial Intelligence Initiative Act, una ley que buscó establecer una estructura más completa para supervisar el desarrollo de esta tecnología. A través de esta normativa, se crearon varias agencias enfocadas en la investigación y regulación de la IA, además de promover la cooperación internacional para impulsar su avance. Sin embargo, a pesar de las buenas intenciones, esta ley no cubre de manera integral los desafíos éticos y legales que la IA plantea. Su enfoque está más centrado en fomentar la investigación y acelerar su aplicación en los sectores económicos y societarios, pero deja de lado la creación de límites claros para proteger derechos fundamentales. En este sentido, la ley carece de un enfoque regulatorio sólido que ponga énfasis en salvaguardar a los individuos frente a los posibles riesgos que la Inteligencia Artificial pueda provocar (Rodríguez Cardona, 2023).

En adición, la Blueprint for an AI Bill of Rights, emitida por la Casa Blanca en 2022, ofrece una serie de principios destinados a guiar el uso ético de la IA, tales como la protección de la privacidad o las medidas contra la discriminación algorítmica, etc. Aunque esta guía no tiene carácter legislativo, proporciona una orientación importante sobre cómo deberían abordarse los problemas relacionados con la IA. Sin embargo, la falta de una ley federal consolidada ha llevado a que algunos estados, como Illinois, promulguen sus propias leyes, como la Ley de Privacidad Biométrica, la cual, como su nombre lo indica, protege datos biométricos, incluyendo huellas dactilares, escaneos de iris, y datos de reconocimiento facial. Esta ley ha resultado en litigios contra grandes empresas tecnológicas como Facebook, Google, y TikTok, debido a violaciones de privacidad relacionadas con la recopilación y almacenamiento no autorizado de datos biométricos (Flórez Rojas & Camelo Pimienta, 2023).

La regulación de la inteligencia artificial (IA) en la República Popular de China, sigue un enfoque estratégico, puesto que existe normativa específica acerca de la IA aplicada en distintas ramas. Desde marzo de 2022, con la implementación del Reglamento de Recomendación de Algoritmos, el gobierno ha establecido normativas que supervisan el desarrollo de la IA, incluyendo el reciente Reglamento de Síntesis Profunda, que obliga a los proveedores a registrar sus algoritmos y a realizar revisiones de seguridad. Estas medidas también requieren que se divulgue el contenido generado por IA y los datos utilizados en su entrenamiento, buscando equilibrar el avance tecnológico con la protección de los derechos de los usuarios (Pérez-Ugena Coromina, 2024).

Aunque China ha abordado la regulación de la Inteligencia Artificial a través de leyes específicas para áreas como la recomendación de algoritmos y los deepfakes, el Consejo de Estado está preparando una ley integral que abarcará todos los aspectos de esta tecnología. Esta futura legislación tiene el potencial de transformar el marco regulatorio del sector, buscando un equilibrio entre fomentar la innovación y garantizar una adecuada protección de los datos personales. Actualmente, las empresas chinas de IA operan cumpliendo con diversas normativas que no solo les otorgan una ventaja competitiva en términos de regulación y adaptación, sino que también fortalecen el control del Estado sobre la información y la expresión en el entorno digital. Este enfoque dual, que impulsa tanto el crecimiento tecnológico como el control gubernamental, refleja la estrategia de China para liderar en IA mientras preserva su modelo de gobernanza en línea (Pérez-Ugena Coromina, 2024).

La Unión Europea ha tomado la delantera en la regulación de la inteligencia artificial con la propuesta de la "AI Act", aprobada en 2024. Esta legislación se convierte en la primera en establecer un marco normativo integral que no solo aborda la seguridad de la inteligencia artificial, sino que también se centra en la protección de datos y los derechos fundamentales de los ciudadanos. Con esta iniciativa, la Unión Europea busca asegurar que el desarrollo y uso de la inteligencia artificial se realice de manera responsable y ética, reflejando su compromiso con los derechos humanos y la dignidad individual.

**Tabla 1**  
*Normativa AI Act*

¿Qué Regula?	Ámbito de Aplicación	Objetivos del Reglamento
El reglamento de la IA de la Unión Europea, conocida como la AI Act, regula el desarrollo, comercialización, implementación y uso de sistemas de inteligencia artificial dentro del Espacio Económico Europeo. Busca regular los usos de la IA para limitar los riesgos que se derivan de estos sistemas.	Se aplica a: <ol style="list-style-type: none"> <li>1. Proveedores de sistemas de IA que ofrezcan productos o servicios basados en IA en la UE, independientemente de si se desarrollaron dentro o fuera de la UE.</li> <li>2. Usuarios que utilicen sistemas de IA en la UE.</li> <li>3. Entidades fuera de la UE cuyos sistemas de IA afecten directa o indirectamente a ciudadanos o usuarios de la UE.</li> </ol>	Los objetivos principales del AI ACT son: Promover el desarrollo y uso seguro de sistemas de IA; Prevenir riesgos que amenacen derechos fundamentales, la seguridad y la salud pública; Establecer confianza en el uso de la IA mediante la creación de un marco legal transparente y preventivo, al estar un paso antes de cualquier situación de riesgo que estas inteligencias pudiesen plantear.

*Nota: Cuadro descriptivo acerca de la nueva normativa implementada por la Unión Europea la “AI Act”.*

Fuente: Basado en EU Artificial Intelligence Act (2024)

Este hito representa un avance significativo en el ámbito de la regulación de la IA, destacando la importancia de alinear el desarrollo tecnológico con valores éticos y legales. La normativa clasifica las aplicaciones de IA según su nivel de riesgo, prohibiendo aquellas consideradas inaceptables, y estableciendo requisitos estrictos para sistemas de alto riesgo, como, por ejemplo, aquellos utilizados en vigilancia y reclutamiento. Esta regulación no se ha desarrollado desde cero; en cambio, se ha construido sobre la base de principios éticos previamente establecidos por la Unión Europea, los cuales se encuentran plasmados en las "Ethics Guidelines for Trustworthy AI" implementadas en 2019. Estas directrices enfatizan la necesidad de aplicar los principios de supervisión humana, robustez técnica, protección de datos, transparencia, equidad, bienestar social y ambiental y rendición de cuentas. De este modo, la “AI Act” no solo cimenta un marco regulatorio sólido, sino que también busca guiar la integración de la IA en la sociedad europea, asegurando que la tecnología respete y potencie los derechos y expectativas de los ciudadanos (Ballarin Usieto, 2024).

Como se mencionó con anterioridad, la normativa sobre IA en la UE se construye con un enfoque basado en el riesgo, reconociendo que no todos los sistemas de IA representan la misma amenaza para los derechos y la seguridad de las personas. Así, se

establecen categorías de riesgo que van desde lo aceptable hasta lo prohibido. Este enfoque permite un balance entre la innovación tecnológica y la protección de los derechos fundamentales. Un punto crítico es la prohibición de ciertos sistemas que representan un "riesgo inaceptable", como aquellos que manipulan cognitiva o emocionalmente a personas vulnerables, fomentando comportamientos dañinos o peligrosos. Este tipo de regulación refleja un compromiso con la seguridad pública, donde tecnologías invasivas, como el reconocimiento facial en tiempo real o la puntuación social, están prohibidas debido a sus implicaciones éticas y de derechos humanos (Temas Parlamento Europeo, 2023).

La "AI Act" aborda de manera concreta ciertos sistemas que la Unión Europea considera de alto riesgo y que, por ello, están prohibidos. Algunos ejemplos de estas prohibiciones incluyen:

- a) Evaluación de fiabilidad: Se prohíbe el uso de tecnologías que evalúan la "fiabilidad" de las personas basándose en su comportamiento social o características personales.
- b) Predicción de conducta delictiva: La normativa restringe el uso de inteligencia artificial para predecir si una persona pudiese cometer un delito, basándose únicamente en perfiles de riesgo.
- c) Reconocimiento facial no consensuado: Se prohíbe la creación de bases de datos de reconocimiento facial a partir de imágenes obtenidas sin el consentimiento de los individuos, ya sea de internet o a través de cámaras de seguridad.
- d) Vigilancia biométrica remota: La regulación también bloquea el uso de sistemas de identificación biométrica remota en tiempo real, lo que evita la implementación de una vigilancia masiva e indiscriminada (Miranzo Díaz, 2024).

Por otro lado, la normativa clasifica los sistemas de IA de alto riesgo, como aquellos que afectan a sectores clave, incluyendo la salud, la educación, o el acceso a servicios esenciales, como el sector público en la administración de justicia y procesos democráticos, gestión de migración y control de fronteras, etc. La ley exige una evaluación exhaustiva de estos sistemas antes y después de su lanzamiento, lo que garantiza que su uso no comprometa la seguridad o los derechos de las personas. Este

enfoque preventivo es fundamental en un contexto donde los sistemas de IA pueden influir en decisiones de gran impacto social, como la contratación laboral o la gestión de infraestructuras críticas. Aunque se contemplan excepciones para ciertos sistemas de IA que no presentan una amenaza significativa, estas excepciones están cuidadosamente reguladas y requieren una justificación sólida por parte de los proveedores, lo que subraya la prioridad de proteger a los ciudadanos sobre el avance tecnológico sin control (IBM, 2024).

Un aspecto clave de esta normativa es la protección de datos personales, que se ve constantemente amenazada por el uso indiscriminado de sistemas de IA. La ley es clara al prohibir el uso de IA para la extracción no selectiva de imágenes faciales o datos biométricos, prácticas que podrían vulnerar gravemente el derecho a la privacidad. Estos sistemas, que operan sobre bases de datos masivas y perfiles detallados de las personas, son considerados de alto riesgo por el potencial que tienen de afectar los derechos fundamentales, como el derecho a la protección de datos. La normativa refuerza la importancia de limitar el uso de IA en este ámbito, garantizando que el tratamiento de datos personales esté siempre sujeto a un control riguroso y a mecanismos de transparencia que eviten abusos.

Para asegurar el cumplimiento de la "AI Act," el reglamento establece un sistema de sanciones que varía en función de la gravedad de las infracciones. Entre las más severas, el reglamento impone multas de hasta 35 millones de euros, aplicables a usos de IA estrictamente prohibidos, como se especifica en el artículo 5. Este nivel de sanción refleja la prioridad de la Unión Europea por evitar prácticas que podrían comprometer derechos fundamentales o la seguridad pública. Las infracciones de nivel intermedio se aplican a los incumplimientos en sistemas de alto riesgo y contemplan sanciones de hasta 15 millones de euros. Este tipo de infracciones incluye, por ejemplo, el incumplimiento de obligaciones de transparencia y los requisitos que deben seguir los proveedores y distribuidores de sistemas de IA en la UE. Finalmente, las infracciones más leves, que se sancionan con hasta 7,5 millones de euros, abarcan prácticas como la presentación de información incorrecta o incompleta. A través de este esquema de sanciones, se evidencia la severidad y magnitud de las multas impuestas, reflejando la intención de la Unión Europea de asegurar el cumplimiento riguroso de la "AI Act" (Miranzo Díaz, 2024).

En definitiva, la Unión Europea se posiciona como líder global en la regulación de la inteligencia artificial, marcando un camino claro hacia el uso responsable y ético de

esta tecnología. A través de un enfoque integral que clasifica los riesgos y establece prohibiciones concretas, la UE ha logrado crear un marco normativo más claro, específico y completo, que protege los derechos fundamentales de los ciudadanos, como la privacidad y la protección de datos personales, sin frenar la innovación tecnológica. Al abordar de manera preventiva los riesgos asociados con la IA y actualizando constantemente su regulación, la UE no solo establece un estándar a nivel regional, sino que también se convierte en un referente para otras jurisdicciones que buscan equilibrar el desarrollo tecnológico con la salvaguarda de los derechos humanos.

## **2.2 Implicaciones Éticas sobre el uso de la IA, en la recopilación, procesamiento y uso de datos personales**

La Inteligencia Artificial no solo ha crecido exponencialmente, trayendo consigo nuevas oportunidades y beneficios a la sociedad a nivel mundial, sino también grandes desafíos éticos, especialmente en lo que respecta a la protección de los datos personales en entornos digitales como el metaverso. Esta iniciativa tecnológica, que permite la inmersión completa en mundos virtuales, plantea cuestiones cruciales sobre cómo se recopilan y utilizan los datos. En particular, se necesita un enfoque sólido de protección de datos para evitar la explotación indebida de la información personal, ya que los entornos virtuales, mediante dispositivos avanzados, pueden capturar datos biométricos y de comportamiento. Esta realidad que nos afecta hoy en día exige un marco legal más fuerte que ponga a la privacidad de los usuarios en el centro de cualquier innovación tecnológica (Terrón Santos, 2022).

Cabe recalcar que cuando se habla de recopilación de datos biométricos, estos no son solo obtenidos de manera virtual, es decir a través de un computador o un teléfono móvil; Actualmente, en las calles, se puede observar un nuevo tipo de estafa, en la cual, con un dispositivo, capturan una fotografía del iris de las personas a cambio de una cantidad de dinero. Con este tipo de información, al ser un dato biométrico, como la huella dactilar o la voz pueden usarlo para robar información personal, como acceder a cuentas bancarias, redes sociales, etc. Es por este claro ejemplo que sucede hoy en día, que se necesita una cultura ética-digital dentro de la sociedad, puesto que, al ser un tema tan reciente, la mayoría de las personas no entienden la magnitud del problema.

La ética digital en estos nuevos espacios virtuales debe priorizar la creación de herramientas que protejan activamente los derechos de los usuarios desde el diseño de

estas tecnologías. Es imperativo que la protección de los datos no sea una opción posterior, sino un elemento básico en la arquitectura de estos sistemas. Esta perspectiva ética es necesaria para evitar que existan abusos masivos de datos, que podría tener consecuencias devastadoras tanto a nivel individual como colectivo. Asimismo, es crucial que las plataformas ofrezcan a los usuarios control total sobre su información personal, de manera que puedan decidir qué datos compartir y con quién (Villalba, 2020).

Por otro lado, cuando existe recopilación masiva de datos biométricos y de comportamiento, esto introduce una nueva serie de riesgos dentro de la ética digital, puesto que hay constantemente un monitoreo de actividad física y emocional de los usuarios, creando así un escenario perfecto para que exista explotación comercial a través de técnicas como el neuromarketing, que estudian las reacciones psicológicas de las personas con la información que obtienen a través de dichos datos. Esta situación es alarmante, puesto que no se está respetando su derecho a la protección de datos ni tampoco su autonomía, pues estaría existiendo una manipulación subconsciente y limitando la capacidad de elegir de la persona, causando consecuentemente inquietudes acerca del uso ético de estas tecnologías (Terrón Santos, 2022).

Existen muchas maneras en las que la Inteligencia Artificial puede vulnerar derechos fundamentales, entre esos derechos, el derecho a la protección de datos personales, rebasando así cualquier uso responsable y ético de estos sistemas. Si bien existen creadores de sistemas inteligentes que priorizan la seguridad y protección de los datos de sus usuarios, basándose en principios fundamentales como la transparencia, el consentimiento, tratamiento de información personal, etc.; lamentablemente no todos comparten esta preocupación e ignoran que el ser humano debe ser el eje fundamental para la creación de su diseño. Esta brecha ética en la creación de sistemas inteligentes pone en riesgo la confianza y la integridad de los usuarios, enfatizando nuevamente la necesidad de crear conciencia de una ética digital.

### **2.3 Estudio de Casos sobre la vulneración del derecho de protección de datos personales por sistemas de IA**

En el subcapítulo anterior, se exploraron las implicaciones éticas del uso de la inteligencia artificial (IA) y cómo esta tecnología ha llegado a vulnerar derechos fundamentales en diversas circunstancias. Sin embargo, para comprender verdaderamente la magnitud de este problema, es necesario profundizar en ejemplos concretos de la vida

real, donde las transgresiones a los derechos humanos y a la privacidad han sido evidentes. A través de casos emblemáticos, se puede tener una visión más crítica acerca de lo que puede llegar a suceder si no se tiene un correcto desarrollo normativo con un enfoque en el ser humano y sus derechos.

Uno de los casos más sonados a nivel mundial, es el famoso caso “Cambridge Analytica”, el cual estalló en 2018, cuando investigaciones periodísticas revelaron que la empresa británica había recopilado datos personales de millones de usuarios de Facebook sin su consentimiento. Cambridge Analytica, que se especializaba en campañas electorales, utilizó estos datos para desarrollar perfiles psicográficos con el fin de influir en elecciones clave, como las presidenciales de Estados Unidos en 2016 y el referéndum del Brexit. La información fue obtenida mediante una aplicación de cuestionarios en Facebook, la cual no solo recolectaba datos de los usuarios que interactuaban con ella, sino también de sus amigos en la red social. Esto permitió que Cambridge Analytica accediera a los datos de hasta 87 millones de personas, exponiendo una falla masiva en la protección de los derechos de privacidad (Vercelli, 2018).

El escándalo sacudió a Facebook y a otras empresas tecnológicas, ya que se demostró cómo los datos personales podían ser explotados sin la autorización directa de los usuarios. Cambridge Analytica utilizó estos datos para personalizar mensajes políticos, manipulando la percepción pública a través de anuncios segmentados. La información recolectada, que incluía datos demográficos, preferencias y comportamientos, fue empleada para influir en decisiones electorales clave, lo que generó serias preocupaciones sobre la transparencia y la ética en el uso de datos con fines políticos. Esta situación evidenció los riesgos de permitir que empresas de marketing político utilicen tecnologías de inteligencia artificial para manipular el comportamiento electoral a gran escala (Vercelli, 2018).

Este caso mostró de manera contundente cómo la recolección y el uso indebido de datos pueden tener implicaciones profundas para la democracia y la protección de los derechos individuales. Las acciones de Cambridge Analytica no solo violaron la privacidad de millones de personas, sino que también expusieron la vulnerabilidad de los sistemas de datos personales ante el abuso por parte de terceros con fines comerciales o políticos. Esto puso de relieve la importancia de establecer regulaciones más estrictas y de exigir mayor responsabilidad a las empresas tecnológicas en la gestión de los datos de los usuarios.

A partir de este escándalo, se ha generado un debate global sobre la necesidad de mejorar los marcos legales para la protección de datos personales y la regulación de los sistemas de inteligencia artificial. La falta de transparencia y control sobre cómo se usan los datos de los usuarios plantea un riesgo grave para los derechos fundamentales, lo que exige una revisión urgente de las políticas de privacidad y un refuerzo de las medidas de protección para evitar futuras violaciones similares.

Otro caso de renombre es el caso Google vs España, también conocido como el caso Google vs la Agencia Española de Protección de Datos (AEPD) y Mario Costeja, es un hito en la jurisprudencia europea, ya que estableció el llamado "derecho al olvido". Mario Costeja González inició este proceso porque en 1998 el diario "La Vanguardia" publicó un anuncio sobre una subasta de bienes de su propiedad debido a que Costeja tenía varias deudas relacionadas con la Seguridad Social. A pesar de que la publicación era legal y necesaria en su momento, al digitalizarse el archivo histórico del periódico, esa información se volvió fácilmente accesible mediante una búsqueda en Google, afectando la reputación de Costeja años después. Ante la negativa de Google y "La Vanguardia" a eliminar la información, Costeja presentó una reclamación ante la AEPD, lo que desencadenó el caso (Martínez Otero, 2015).

Uno de los puntos clave que surgió en este litigio fue determinar si la normativa española de protección de datos era aplicable a una empresa como Google, cuya sede principal está fuera de Europa. En su defensa, Google argumentó que su servicio de motor de búsqueda no estaba sujeto a las leyes españolas, ya que operaba desde Estados Unidos. Sin embargo, el Tribunal de Justicia de la Unión Europea (TJUE) determinó que la normativa española era aplicable, dado que Google Spain, su filial local, gestionaba la publicidad relacionada con las búsquedas en España, lo que vinculaba su actividad comercial con el tratamiento de datos personales en territorio europeo (Martínez, 2017).

Otro aspecto significativo fue la responsabilidad de Google en cuanto al tratamiento de datos personales. Mientras que Google sostenía que simplemente indexaba información disponible públicamente sin tener control sobre su contenido, el TJUE concluyó que, al organizar, almacenar y presentar esa información, Google también era responsable de su tratamiento. El tribunal consideró que los buscadores tienen un impacto significativo en la difusión de datos y que, en este contexto, el derecho a la protección de datos personales y al honor del afectado debe prevalecer sobre los intereses comerciales de las empresas tecnológicas (Martínez, 2017).

Finalmente, el Tribunal de Justicia de la Unión Europea (TJUE) reconoció el derecho de los individuos a solicitar la eliminación de enlaces que conduzcan a información obsoleta o irrelevante sobre ellos. Este derecho, conocido como el derecho al olvido, no implica borrar la información de su fuente original, como en el caso de "La Vanguardia", sino que se refiere específicamente a su desindexación en los resultados de búsqueda que están asociados al nombre de una persona. Así, aunque la noticia podía permanecer de manera accesible en el archivo digital del periódico, Google debía eliminar los enlaces que la relacionaran directamente con el nombre de Costeja, lo que permite a los individuos ejercer un mayor control sobre su imagen y reputación en línea.

El fallo del TJUE en este caso fue un paso importante para consolidar los derechos de protección de datos personales en la era digital, estableciendo que los motores de búsqueda deben equilibrar el derecho a la información con el derecho a la privacidad de los individuos. Desde entonces, Google ha implementado un mecanismo para que los usuarios soliciten la eliminación de enlaces en situaciones similares, aunque cada solicitud se analiza en función de la relevancia y el interés público de la información en cuestión.

A raíz de este caso, resulta pertinente profundizar en el derecho al olvido, ya que está estrechamente vinculado con salvaguardar el derecho de protección de datos personales. En la actualidad, cualquier persona con información en la web puede ser fácilmente localizada a través de búsquedas en línea, lo que permite acceder a sus datos. Un ejemplo claro puede ser la búsqueda de información sobre una persona que se encuentra en la política; en estos casos, es posible encontrar tanto datos recientes como contenidos antiguos, los cuales pueden ser útiles o, en algunos casos, perjudicar la reputación de esa persona. Esta realidad, en un entorno cada vez más dependiente de las redes y el internet, convierte a la información en una herramienta de doble filo, donde los derechos de protección de datos son frecuentemente vulnerados, y los usuarios, en su mayoría, no son conscientes del alcance de dicha exposición.

Una persona tiene el derecho de solicitar la eliminación o limitación de ciertos datos cuando estos resulten ser impertinentes, excesivos o, en cualquier caso, atenten contra su reputación o dignidad por diversas razones. Esta solicitud es particularmente pertinente cuando la información en cuestión ha perdido su utilidad y veracidad a lo largo del tiempo, lo que puede llevar a la difusión de datos erróneos o perjudiciales. Sin embargo, es fundamental que dicha petición se realice con la debida consideración de que la

información que se desea eliminar no infrinja el derecho a la información pública. Esto implica un delicado equilibrio entre la protección de los derechos individuales y el interés general en la transparencia y acceso a la información. Por lo tanto, se debe evaluar cuidadosamente cada caso para garantizar que se respeten ambos principios, sin menoscabar la integridad de la información pública (Oscar Puccinelli, 2019).

No obstante, el derecho al olvido se ha vuelto una herramienta valiosa en la era digital e inteligente en la que vivimos, permitiendo a las personas solicitar la eliminación de información personal que ya no es relevante o que resulta perjudicial, como lo demuestra el caso del señor Costeja. Aun así, la falta de conocimiento de la norma ha mantenido al margen a muchas personas, lo que les impide proteger adecuadamente su privacidad y ejercer sus derechos en un entorno donde la información personal puede ser fácilmente accesible y utilizada sin su consentimiento.

Aunque no está regulado de manera explícita en nuestra legislación interna, se refleja implícitamente en la Ley de Protección de Datos Personales, que contempla la rectificación y eliminación de datos desactualizados o incorrectos. A pesar de no estar plenamente desarrollado en nuestro marco jurídico, este derecho ofrece una vía para proteger la información personal en el entorno digital, destacando la necesidad de que más personas conozcan sus beneficios y posibilidades.

## **CAPÍTULO 3**

### **3. PROPUESTAS Y RECOMENDACIONES A REGLAMENTOS PREVIAMENTE ANALIZADOS**

Como se ha examinado en capítulos previos, se evidencia de manera clara que, tanto a nivel internacional como en el ámbito nacional, persisten deficiencias significativas en la formulación de normativas destinadas a la regulación de la Inteligencia Artificial. Estas fallas se manifiestan ya sea en la ausencia de regulaciones específicas o en la existencia de marcos normativos insuficientes que no abordan adecuadamente la protección de derechos fundamentales que pueden verse comprometidos por el uso de estas tecnologías, tales como la protección de los datos personales. En consecuencia, este capítulo tiene como objetivo proponer ideas y recomendaciones orientadas a mejorar las normativas existentes o, en su defecto, establecer directrices iniciales para el desarrollo de una regulación adecuada cuando estas aún no estén presentes.

#### **3.1 Ecuador**

En el contexto ecuatoriano, como se ha mencionado previamente, si bien existe una Ley Orgánica de Protección de Datos Personales que busca salvaguardar este derecho, reconocido hoy en día como un bien jurídico protegido en nuestra legislación, dicha normativa aún presenta limitaciones que no permiten satisfacer plenamente las necesidades actuales.

Entre las principales deficiencias de la normativa actual, destaca la omisión de regular adecuadamente la posible vulneración del derecho a la protección de datos por parte de tecnologías avanzadas, como la Inteligencia Artificial, que operan con extensas bases de datos. Esta situación genera serias dudas sobre la efectividad de la ley, dado que no aborda de manera explícita el manejo masivo de información personal por parte de estas tecnologías. La ausencia de disposiciones claras sobre el uso indebido o la filtración de datos por sistemas de IA revela un vacío legal que exige atención urgente. Este escenario resalta la necesidad de reformar o complementar el marco normativo vigente, con el fin de asegurar una protección más integral y adaptada a los desafíos actuales que representan estas innovaciones tecnológicas.

Desde una perspectiva personal, no solo es fundamental reforzar la Ley Orgánica de Protección de Datos Personales, aunque esta representa un paso inicial necesario. En el contexto actual, marcado por el rápido avance tecnológico, resulta imperativo desarrollar una normativa específica que regule de manera integral la Inteligencia Artificial. Esta tecnología abarca múltiples aspectos que requieren ser controlados y limitados. Uno de los enfoques prioritarios de dicha regulación debe ser la protección de los datos personales, limitando el acceso de las IA a la información de los usuarios, pero más allá de eso, controlando estrictamente el uso y tratamiento que se da a esos datos. Con frecuencia, una vez recolectada la información, no existen mecanismos adecuados para garantizar su protección, lo que se agrava ante la falta de una regulación clara que establezca las obligaciones y límites en el manejo de estos datos.

En la actualidad, la Inteligencia Artificial es conceptualizada como objeto de derecho; sin embargo, su rápido crecimiento y creciente autonomía han generado debates sobre si debería ser reconocida como sujeto de derecho, lo que implicaría no solo la adquisición de derechos, sino también de obligaciones (Coka Flores & Portilla Obando, 2023). Dado el constante dinamismo del panorama tecnológico, es importante que los marcos jurídicos evolucionen y se adapten a las nuevas realidades y desafíos que plantea el desarrollo de la IA. Esto nos lleva a cuestionar hasta qué punto es sostenible permitir que la IA continúe operando sin una regulación consolidada, ya que la falta de un control adecuado podría seguir facilitando la vulneración de derechos fundamentales.

Si se considera la posibilidad de crear una normativa que regule la Inteligencia Artificial (IA) en Ecuador con un enfoque en la protección de datos personales, es fundamental que esta ley comience por establecer definiciones claras de términos esenciales como IA, datos personales y el tratamiento de estos. Esto ayudará a asegurar que la aplicación de la normativa sea consistente y efectiva. Además, es crucial que se delimite el ámbito de aplicación de manera precisa, abarcando tanto el sector público como el privado, para que ninguna actividad relacionada con el manejo de datos quede fuera del alcance de la regulación. También es vital que se reconozcan y protejan los derechos de los titulares de los datos, como el acceso, la rectificación, la cancelación y la oposición al tratamiento de su información personal.

Asimismo, la ley debe imponer obligaciones estrictas a aquellos que manejan datos, garantizando medidas de seguridad, promoviendo la transparencia en los procesos y estableciendo la obligación de notificar cualquier incidente que pueda comprometer la

integridad de la información. Es importante recordar que detrás de las tecnologías de IA hay seres humanos que las desarrollan, por lo que deben asumir la responsabilidad de su correcto funcionamiento y mantenerlas en constante actualización para que no se vulneren los derechos fundamentales de los usuarios.

Por otro lado, la regulación también debe abordar de forma integral el uso de la IA en sectores críticos como la salud, las finanzas, la educación y la seguridad nacional, donde el tratamiento de datos es especialmente delicado. Para ello, la ley debería incluir estándares internacionales de seguridad, como el cifrado de datos y técnicas de anonimización que ayuden a reducir los riesgos asociados con el manejo de grandes volúmenes de información personal.

Algo se suma importancia, es educar y concientizar a la gente, promoviendo el uso de sistemas que sean transparentes y fáciles de entender. Esto permitiría a los usuarios conocer cómo se toman las decisiones automatizadas que pueden influir en sus derechos, de esta manera se estaría garantizando un uso responsable de la IA. Para asegurar que la normativa se cumpla efectivamente, es necesario crear un organismo encargado de auditar y supervisar las prácticas de IA en el país. Este ente deberá tener la capacidad de fiscalizar y garantizar que se respeten las disposiciones establecidas, así como de aplicar sanciones justas y ofrecer mecanismos de reparación cuando se produzcan infracciones.

La creación de esta regulación no debe ser un proceso aislado; al contrario, debe surgir de un diálogo abierto y participativo. Es así, que involucrar a expertos en inteligencia artificial, así como a representantes del sector público y privado, enriquecerían el proceso con sus diferentes perspectivas. De esta manera, se podrá construir una normativa que no solo sea completa y equilibrada, sino que también responda de manera efectiva a los retos tecnológicos que enfrentamos en la actualidad.

Ecuador se encuentra rezagado en comparación con países como aquellos que conforman la Unión Europea, donde ya se han establecido directrices claras sobre cómo debe desarrollarse una legislación adecuada en materia de Inteligencia Artificial (IA). La Unión Europea se destaca como el mejor ejemplo a seguir, ya que ha avanzado significativamente en la regulación de esta tecnología, lo que ofrece una referencia invaluable para otros países que aún están en proceso de definir sus marcos legales. Es imperativo que Ecuador siga estos pasos antes de que el avance continuo de la tecnología profundice aún más nuestra desventaja.

A pesar de que existen iniciativas legislativas, como las propuestas por las legisladoras Karina del Carmen Subia y Patricia Núñez, estas aún no abordan de manera integral los aspectos fundamentales que debería incluir una regulación efectiva de la IA en el país. La falta de una normativa clara y precisa expone a Ecuador al riesgo de quedar rezagado en el desarrollo tecnológico global, limitando no solo la competitividad, sino también la protección adecuada de los derechos de los ciudadanos frente a los desafíos que presenta la IA.

Si bien es esencial que cualquier normativa contemple la protección de los datos personales frente a los posibles abusos de la inteligencia artificial, también es importante que dicha regulación no frene el desarrollo de esta tecnología. Se debe buscar un equilibrio que permita proteger los derechos fundamentales sin sofocar el avance de la innovación. Establecer demasiadas restricciones podría obstaculizar el potencial de la IA y limitar las oportunidades de crecimiento en este ámbito. Por lo tanto, la legislación debe garantizar que se respeten los derechos fundamentales, la seguridad y ética del uso y aplicación de la IA, pero sin imponer barreras que impidan su progreso, permitiendo así que Ecuador se mantenga competitivo y alineado con la evolución tecnológica a nivel global.

### **3.2 Estados Unidos**

Como se mencionó en el capítulo 2, la regulación de la inteligencia artificial (IA) en Estados Unidos presenta deficiencias significativas. Utilizo el término "deficiente" para describir este estado, ya que el país no ha logrado establecer una ley que abarque de manera integral todos los aspectos relacionados con la regulación de la IA, a medida que esta tecnología ha evolucionado con el tiempo. Esto es particularmente notable considerando que Estados Unidos es una nación de primer mundo, conocida por su liderazgo en múltiples áreas y su capacidad para adaptarse rápidamente a las necesidades cambiantes de sus ciudadanos. Sin embargo, en este caso específico, el país no sirve como ejemplo a seguir, lo que genera preocupaciones sobre la forma en que se abordan los desafíos asociados a la inteligencia artificial.

Uno de los mayores problemas que enfrenta Estados Unidos en este aspecto es la fragmentación normativa entre los estados. En lugar de una ley federal que establezca pautas claras y uniformes para el desarrollo y uso de la IA en todo el país, cada estado ha creado sus propias regulaciones. Esto ha dado lugar a un mosaico de normativas que no

solo dificultan la aplicación efectiva de la ley, sino que también generan incertidumbre tanto para las empresas como para los ciudadanos. Un ejemplo destacado es la Ley de Privacidad Biométrica de Illinois, que, aunque es un esfuerzo importante para proteger la privacidad, refleja la disparidad de enfoques a nivel estatal. Mientras que algunos estados avanzan en la regulación, otros permanecen rezagados, lo que crea un entorno normativo inconsistente.

Por esta razón, se considera fundamental la creación de una normativa federal integral que aborde de manera exhaustiva todos los aspectos de la inteligencia artificial. Aunque han existido algunas regulaciones a nivel federal, estas han sido ambiguas y poco completas, lo que ha generado una falta de claridad en la aplicación de las leyes. Al mismo tiempo, cada estado ha intentado desarrollar sus propias leyes, pero estas iniciativas suelen ser reactivas y limitadas, enfocándose principalmente en preocupaciones locales sin tener en cuenta el panorama general. Una normativa federal unificadora no solo podría resolver esta fragmentación, sino que también serviría para combinar las mejores prácticas y enfoques ya implementados en diversos estados, como la ley de Illinois sobre privacidad biométrica.

Al igual que se recomendó para Ecuador, la legislación integral de Estados Unidos debería establecer estándares claros y consistentes para la regulación de la IA en todo el país, garantizando un desarrollo tecnológico ético y responsable. A diferencia de Ecuador, Estados Unidos cuenta con normativas como la National Artificial Intelligence Initiative Act, enfocada principalmente a fomentar la investigación y promover el avance de la inteligencia artificial. Si bien esta ley es un paso positivo para impulsar el desarrollo de la IA, también es necesario, como se recomendó para Ecuador, lograr un equilibrio adecuado. No basta con promover el avance tecnológico; es fundamental que la legislación no se limite únicamente a esto, sino que también aborde rigurosamente aspectos como las sanciones, las limitaciones y los posibles riesgos que podrían surgir.

Asimismo, esta normativa debe incluir una sólida protección de los derechos fundamentales, con especial énfasis en la protección de los datos personales, que es uno de los mayores retos en la era digital. Este equilibrio es necesario para garantizar que, aunque se continúe incentivando el desarrollo tecnológico, se implementen mecanismos claros y efectivos para mitigar los riesgos inherentes al uso de la IA, protegiendo así a los ciudadanos y su información personal.

Además, Estados Unidos tiene la oportunidad de liderar a nivel global en la creación de normas que regulen la inteligencia artificial dentro de un marco ético y legal sólido. Como pionero en innovación tecnológica, el país debe esforzarse por establecer estándares que no solo protejan a los ciudadanos, sino que también promuevan el desarrollo responsable y sostenible de la inteligencia artificial. Al hacerlo, Estados Unidos puede servir como modelo para otras naciones, demostrando que es posible equilibrar la innovación con la protección de los derechos individuales y la ética. En un mundo cada vez más digitalizado y dependiente de la tecnología, es importante que el país no se quede atrás en este ámbito, sino que tome la delantera en la regulación adecuada de la IA, asegurando un futuro donde los beneficios de esta tecnología se puedan disfrutar de manera equitativa y segura para todos.

### **3.3 China**

China, se ha destacado por implementar una normativa clara y sólida en el ámbito de la inteligencia artificial (IA), abordando de manera exhaustiva la seguridad y privacidad en sus reglamentos. A través de una serie de disposiciones bien definidas, el país ha priorizado el control y la regulación de los algoritmos desde las fases iniciales de desarrollo, sometiéndolos a rigurosas revisiones de seguridad y a múltiples fases de evaluación de control ante el gobierno (Pérez-Ugena, 2024). Como se explicó con anterioridad, estos sistemas deben cumplir con estrictos requisitos de ciberseguridad y procedimientos de registro de información, lo que refleja el compromiso del gobierno chino por establecer un marco regulatorio que brinde confianza y protección tanto a los usuarios como a la sociedad en general.

En este contexto, el Consejo de Estado Chino ha estado trabajando en el diseño de una legislación que se mantenga a la par de las crecientes y cambiantes demandas tecnológicas y sociales. Este esfuerzo pretende seguir el ritmo de la Unión Europea, que también ha implementado marcos regulatorios avanzados para la IA. China busca establecer un equilibrio entre el control de las tecnologías emergentes y el fomento de un ecosistema seguro y ético. Este enfoque, si bien esencial para la estabilidad y el orden, tiende a ser restrictivo, lo cual podría representar un desafío para la innovación.

Desde una perspectiva analítica, aunque es evidente que China ha logrado importantes avances en el control y la seguridad en temas de IA, también podría beneficiarse de un enfoque regulatorio que dé mayor espacio a la innovación y a la

investigación en IA. A diferencia de Estados Unidos, donde las políticas hacia la IA tienden a ser más permisivas y enfocadas en promover el crecimiento del sector, China aún necesita equilibrar sus normativas de control con políticas que fomenten la creatividad y la investigación en tecnologías de IA. Así, la regulación podría transformarse en un facilitador para el desarrollo de nuevas aplicaciones y enfoques en IA que impulsan el conocimiento y el crecimiento tecnológico.

Sería recomendable que cualquier futura normativa en China busque un equilibrio integral. Es fundamental que se asegure la protección de los derechos y la seguridad de los datos, además de imponer sanciones y limitaciones cuando sea necesario. No obstante, también debería promover el uso correcto de la IA, su desarrollo en ámbitos inteligentes y estimular la innovación. De este modo, se lograría un entorno regulatorio que no solo controle los riesgos, sino que también impulse el potencial de la IA en beneficio de la sociedad y el desarrollo científico y tecnológico del país.

Además de esta recomendación, cabe señalar que China está avanzando en la dirección correcta. Aunque su desarrollo normativo en el ámbito de la IA aún tiene margen de crecimiento, es evidente que el país ha priorizado aspectos esenciales como la protección de derechos fundamentales, incluyendo el derecho a la protección de datos personales, la seguridad y la privacidad. Esta orientación representa un importante paso adelante, consolidando una base sólida para el manejo ético y seguro de la inteligencia artificial en su sociedad.

### **3.4 Unión Europea**

La Unión Europea ha demostrado ser líder y pionera en el desarrollo normativo de la inteligencia artificial, estableciendo una sola norma exhaustiva que sirve como modelo para el resto del mundo. No se trata de una regulación con conceptos preliminares y simples, sino de un marco legal completo e integral que cubre múltiples aspectos del desarrollo y uso de la Inteligencia Artificial. Este marco, conocido como la "AI Act," abarca tanto la promoción de innovaciones tecnológicas como las restricciones y medidas de seguridad necesarias para proteger los derechos fundamentales de los ciudadanos.

Como se ha señalado anteriormente, a través de un enfoque basado en el riesgo, esta normativa clasifica los sistemas de IA en distintos niveles de peligrosidad, desde aquellos considerados de "riesgo inaceptable" y que están prohibidos, hasta los de "alto riesgo,"

que deben cumplir con estrictos controles de seguridad y transparencia antes de poder operar.

La "AI Act" representa un avance sin precedentes en la regulación de la inteligencia artificial, marcando un antes y un después en el contexto legislativo a nivel global. Al ser la primera normativa de este tipo, establece un enfoque ejemplar para otros países que aún no han implementado regulaciones similares. Desde una perspectiva de responsabilidad ética y social, esta ley no solo establece normas, sino que también demuestra cómo una legislación en la era digital puede adaptarse a las necesidades actuales, abordando aspectos esenciales como la protección de datos personales, la seguridad y la transparencia en la implementación de IA. Este marco normativo va más allá de controlar la tecnología; también sienta las bases para asegurar que los desarrollos tecnológicos sirvan al bien común y no pongan en riesgo la dignidad o los derechos fundamentales de las personas.

Uno de los puntos más relevantes y que nos compete de la ley, es su énfasis en la protección de datos personales, un valor fundamental en la legislación europea. La AI Act refuerza la importancia de salvaguardar la privacidad de los ciudadanos en cada etapa de desarrollo y uso de la inteligencia artificial, en línea con otras normas clave como el Reglamento General de Protección de Datos (GDPR). De este modo, la AI Act no solo plantea principios éticos, sino que incorpora la protección de datos en el núcleo de la regulación de la IA. Con esta norma, la Unión Europea no solo marca el camino hacia una legislación adaptada a los desafíos de la era digital, sino que también establece un sólido marco de defensa para los derechos fundamentales en una sociedad cada vez más influenciada por la tecnología.

Dada la solidez y la amplitud de ley, no parece necesario hacer ninguna recomendación a la comunidad europea, ya que, como se ha mencionado, han logrado desarrollar un marco regulatorio ejemplar.; Sin embargo, el éxito de esta normativa dependerá en gran medida de su aplicación práctica en los Estados miembros de la Unión Europea. Aunque la AI Act está bien estructurada y detallada en su contenido, el reto principal ahora es asegurar que se aplique de manera efectiva y no se convierta en una normativa de cumplimiento superficial. La implementación efectiva de esta norma no solo requerirá el compromiso de los gobiernos, sino también la colaboración de instituciones, el sector privado y la sociedad civil. Para que la AI Act cumpla su propósito, la Unión Europea debe mantener una supervisión rigurosa y fomentar la colaboración

entre los distintos sectores, garantizando así que las disposiciones de la normativa se traduzcan en una protección real para los ciudadanos.

## CONCLUSIONES

En conclusión, el avance tecnológico ha puesto en evidencia que como sociedad estamos quedándonos atrás en la creación de marcos normativos adecuados para enfrentar los retos del presente. Mientras la tecnología sigue avanzando a pasos agigantados, las regulaciones no han evolucionado al mismo ritmo, lo que ha permitido la vulneración de derechos fundamentales, especialmente en el ámbito de la protección de datos personales. Casos de gran relevancia han mostrado cómo grandes empresas, como Facebook o Google, a través de sus plataformas, han violado de manera significativa estos derechos, afectando a cientos de personas en todo el mundo. En este contexto, la Unión Europea ha demostrado ser pionera en la creación de un marco regulatorio sólido y efectivo, estableciendo un ejemplo que otros países, incluido Ecuador, deberían seguir.

Si bien Ecuador tiene una Ley Orgánica de Protección de Datos Personales, esta legislación aún no aborda de manera específica las vulneraciones que pueden ocurrir a través del uso de inteligencia artificial. Esto revela la necesidad urgente de seguir innovando y de no quedarnos atrás. La experiencia europea ha demostrado que es posible encontrar un equilibrio entre la promoción de la innovación tecnológica y la protección de los derechos fundamentales. La normativa de la Unión Europea no solo fomenta el desarrollo de la inteligencia artificial de manera segura, sino que también establece controles claros para garantizar que, en caso de incumplimientos o vulneraciones, existan sanciones efectivas que protejan a los ciudadanos.

Es esencial que Ecuador, al igual que otros países, siga este ejemplo y continúe fortaleciendo su legislación en esta área, adaptándose a las necesidades actuales y anticipando los desafíos futuros. La inteligencia artificial, como cualquier herramienta poderosa, debe desarrollarse dentro de un marco ético que garantice un progreso tecnológico responsable, asegurando que el avance de la humanidad vaya de la mano con la protección de sus derechos fundamentales. Solo así podremos construir un futuro en el que la tecnología sirva para el beneficio de todos, sin comprometer nuestra privacidad ni nuestra dignidad.

Otro aspecto importante y que debe tomarse en cuenta, es la educación y concientización sobre la inteligencia artificial. En muchas ocasiones, el desconocimiento sobre cómo funcionan estas tecnologías lleva a que las personas cometan errores en su uso o compartan información personal sin entender las implicaciones. Un ejemplo común

es cuando se accede a páginas web, donde, a menudo, se comparten datos sin ser plenamente conscientes de ello, o sin comprender a quién se está entregando esta información y cómo se utilizará. Esta falta de entendimiento no solo incrementa la vulnerabilidad ante posibles abusos por parte de empresas o sistemas inteligentes, sino que también facilita la explotación de los datos sin el consentimiento adecuado. De no promoverse una mayor conciencia sobre los riesgos asociados con el uso de la inteligencia artificial, la exposición a la vulneración del derecho de protección de datos personales seguirá creciendo de manera alarmante. Por tanto, es imprescindible que se impulse una educación integral que permita a la sociedad entender los mecanismos de protección disponibles, identificar los riesgos y asumir las responsabilidades al interactuar con estas tecnologías. Solo a través de una ciudadanía informada podremos mitigar los perjuicios potenciales y garantizar un uso responsable y ético de la inteligencia artificial.

## REFERENCIAS

- Albornoz, M. M. (2021). El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición? *REVISTA IUS*, 15(48). <https://doi.org/10.35487/rius.v15i48.2021.715>
- Arellano López, C. A. (2020). El Derecho de Protección de Datos Personales. *BIOLEX REVISTA JURIDICA DEL DEPARTAMENTO DE DERECHO*, 12(23 jul-dic), 127–136. <https://doi.org/10.36796/biolex.v0i23.194>
- Ballarin Usieto, P. (2024). *Los factores sociales en la construcción de la ética de la Inteligencia Artificial: causas e implicaciones de las estrategias regulatorias de la IA en China, Estados Unidos y la Unión Europea*. <http://hdl.handle.net/10609/151014>
- Cáceres Nieto, E. (2023). LA INTELIGENCIA ARTIFICIAL APLICADA AL DERECHO COMO UNA NUEVA RAMA DE LA TEORÍA JURÍDICA. *Anales de La Cátedra Francisco Suárez*, 57, 63–89. <https://doi.org/10.30827/acfs.v57i.26281>
- Coka Flores, D. F., & Portilla Obando, P. D. (2023). Regulación de la inteligencia artificial: Análisis comparativo de Ecuador y legislaciones internacionales. *Repositorio Institucional UNIANDES*.
- Constitución de La República Del Ecuador (2008).
- Enríquez, O. A. M. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *REVISTA IUS*, 15(48). <https://doi.org/10.35487/rius.v15i48.2021.743>
- EU Artificial Intelligence Act (2024).
- Fernández-Aller, C., & Serrano Pérez, M. M. (2022). ¿Es posible una Inteligencia artificial respetuosa con la protección de datos? *Doxa. Cuadernos de Filosofía Del Derecho*, 45, 307. <https://doi.org/10.14198/DOXA2022.45.11>
- Flórez Rojas, M. L., & Camelo Pimienta, A. M. (2023). Tecnologías de reconocimiento facial en Colombia: Análisis comparativo en relación con la protección de datos. *Ius et Praxis*, 29(1), 3–26. <https://doi.org/10.4067/S0718-00122023000100003>
- Hui, Y. (2017). ¿Qué es un objeto digital? (E. Rueda Hernández & K. Picón Angarita, Trans.). *Virtualis: Revista de Cultura Digital*, 8(15), 81–96. <https://www.revistavirtualis.mx/index.php/virtualis/index>
- IBM. (2024, June 20). *¿Qué es la Ley de Inteligencia Artificial de la Unión Europea (Ley de IA de la UE)?* <https://www.ibm.com/es-es/topics/eu-ai-act>

- IEEE, & Ministerio de Defensa. (2017). La inteligencia artificial aplicada a la defensa. In IEEE & Ministerio de Defensa (Eds.), *Documentos de Seguridad y Defensa* (Issue 79).
- León Carvajal, M. C. (2009). *Derecho a la protección de datos personales y la seguridad informática* [UniversidadDelAzuay]. <http://dspace.uazuay.edu.ec/handle/datos/871>
- Machuca Vivar, S. A., Vinueza Ochoa, N. V., Sampedro Guamán, C. R., Santillán Molina, A. L., Machuca Vivar, S. A., Vinueza Ochoa, N. V., Sampedro Guamán, C. R., & Santillán Molina, A. L. (2022). HABEAS DATA Y PROTECCIÓN DE DATOS PERSONALES EN LA GESTIÓN DE LAS BASES DE DATOS. *Revista Universidad y Sociedad*, 14(2). [http://scielo.sld.cu/scielo.php?pid=S2218-36202022000200244&script=sci\\_arttext&tlng=pt](http://scielo.sld.cu/scielo.php?pid=S2218-36202022000200244&script=sci_arttext&tlng=pt)
- Martínez, J. (2017). LA APLICACIÓN DEL DERECHO AL OLVIDO EN ESPAÑA TRAS LA STJUE GOOGLE CONTRA AEPD Y MARIO COSTEJA. *Iuris Tantum Revista Boliviana de Derecho*, 23(23).
- Martínez Otero, J. M. (2015). El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja. *Revista de Derecho Político*, 93. <https://doi.org/10.5944/rdp.93.2015.15139>
- Miranzo Díaz, J. (2024). *El Reglamento de Inteligencia Artificial de la UE: regulación de riesgos y sistemas de estandarización (The EU Artificial Intelligence Act: Risk Regulation and Standardization Systems)*. <https://doi.org/10.2139/ssrn.4911496>
- Núñez Ramos, S. P. (2024). *Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador*.
- Oscar Puccinelli. (2019). El derecho al olvido digital. La nueva cara de un derecho tan viejo como polémico. *Revista Derecho Constitucional | Universidad Blas Pascal*, 1. [https://doi.org/10.37767/2683-9016\(2019\)006](https://doi.org/10.37767/2683-9016(2019)006)
- Parra Sepúlveda, D., & Concha Machuca, R. (2021). Inteligencia artificial y derecho. Problemas, desafíos y oportunidades. *Vniversitas*, 70. <https://doi.org/10.11144/Javeriana.vj70.iadp>
- Pérez-Ugena Coromina, M. (2024). Análisis comparado de los distintos enfoques regulatorios de la inteligencia artificial en la Unión Europea, EE. UU., China e Iberoamérica. *Anuario Iberoamericano de Justicia Constitucional*, 28(1), 129–156. <https://doi.org/10.18042/cepc/aijc.28.05>
- Pérez-Ugena, M. (2024). La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales. *Estudios de Deusto*, 72(1), 307–337. <https://doi.org/10.18543/ed.3108>

- Ponce, J. S., & Espinosa Velarde, C. (2024). Análisis Inicial del nuevo Proyecto de Ley para el Fomento y Desarrollo de la Inteligencia Artificial en Ecuador. *ECIJAGPA*.
- Rodríguez Cardona, M. (2023). Los intentos de regulación de la Inteligencia Artificial: Derecho Comparado entre España, Puerto Rico y Estados Unidos. *Derecom*, 35, 1–19. <http://www.derecom.com/derecom/>
- Rosas-Lanas, G., & Pila-Cárdenas, G. (2023). protección de datos personales en Ecuador. *VISUAL REVIEW. International Visual Culture Review / Revista Internacional de Cultura Visual*, 13(2), 1–16. <https://doi.org/10.37467/revvisual.v10.4568>
- Temas Parlamento Europeo. (2023, June 12). *Ley de IA de la UE: primera normativa sobre inteligencia artificial*. <https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial>
- Terrón Santos, D. (2022). *Metaverso y derecho: implicaciones éticas y jurídicas más allá de los horizontes de la privacidad*.
- Vercelli, A. (2018). La (des)protección de los datos personales: análisis del caso Facebook Inc.- Cambridge Analytica. *Simposio Argentino de Informática y Derecho*, 2, 1–12. <https://www.nytimes.com/>
- Villalba, J. F. (2020). Algor-ética: la ética en la inteligencia artificial. *Anales de La Facultad de Ciencias Jurídicas y Sociales de La Universidad Nacional de La Plata*, 50. <https://doi.org/10.24215/25916386e062>