UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

REFORMA A LA LEY DE DATOS PARA INTEGRAR EL USO Y CONTROL DE IA EN LA GESTION Y PROCESAMIENTO DE DATOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO.

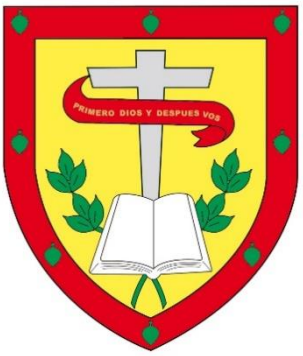
AUTOR: CHRISTIAN ADRIAN CRIOLLO VERA.

DIRECTOR: AB. JUAN PABLO MARTINEZ ALBORNOZ.

CUENCA - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

REFORMA A LA LEY DE DATOS PARA INTEGRAR EL USO Y CONTROL DE IA EN LA GESTION Y PROCESAMIENTO DE DATOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

AUTOR: CHRISTIAN ADRIAN CRIOLLO VERA

DIRECTOR: AB. JUAN PABLO MARTINEZ ALBORNOZ

CUENCA - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Universidad Católica de Cuenca	DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD	CÓDIGO: F – DB – 34 VERSION: 01 FECHA: 2021-04-15 Página 1 de 1

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Christian Adrian Criollo Vera, portador de la cédula de ciudadanía **N° 0105755185,** Declaro ser el autor de la obra: **"Reforma a la ley de datos para integrar el uso y control de IA en la gestión y procesamiento de datos.",** sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, 22 de mayo del 2025

F.....

Christian Adrian Criollo Vera

C.I 0105755185

CERTIFICADO DE AUTORÍA

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente Trabajo de Investigación fue desarrollado por **Christian Adrian Criollo Vera**, con el tema **"Reforma a la ley de datos para integrar el uso y control de IA en la gestión y procesamiento de datos."**, bajo mi supervisión.

F: .....

Dr. Juan Pablo Martínez Albornoz. Mgs
Docente - Tutor

DEDICATORIA

A Dios, por ser la luz que ilumina mi sendero
y la fuerza que sostiene mi espíritu en cada desafío.
Gracias por otorgar la sabiduría para discernir, la resiliencia
para avanzar y la paz que habita en mi corazón a lo largo de este camino.
A mis amados padres, Guilmer Criollo y Rosa Vera, mi más sólido pilar
y mi mayor inspiración. Su amor incondicional, su inalcanzable
dedicación y su inquebrantable fe en mí han sido la
base sobre la que he construido cada logro. Gracias por cada sacrificio
silencioso, por cada enseñanza de mi vida y por ser el refugio donde siempre
encuentro fortaleza y amor. Este triunfo es tan suyo como mío.
A mis abuelos, a mi tía Patricia Vera, a mi prima Evelyn Vintimilla,
a mi amigo y mentor Padre Eduardo Martínez, gracias por su amor infinito,
su paciencia inagotable y su confianza absoluta y mi capacidad. Gracias por
recordarme, en los momentos de duda, la fortaleza que reside en mí
y el horizonte inmenso que tengo por delante. Cada palabra de aliento,
cada abrazo sincero y cada instante compartido
ha sido mi mayor Aliciente en este proceso.
A mi tutor, Dr. Juan Pablo Martínez, por su invaluable orientación,
por su confianza y mis capacidades y por ser un guía especial en este proceso.
Su conocimiento, paciencia y compromiso han sido
determinantes en la culminación de este trabajo,
y por ello lo estaré siempre agradecido.

Con profunda gratitud y cariño, gracias por ser
parte de este proceso y sueño hecho realidad.

RESUMEN

El presente trabajo de investigación examina la necesidad imperante de reformar el marco jurídico ecuatoriano en materia de protección de datos personales, con el propósito de integrar de manera efectiva el uso y control de la inteligencia artificial (IA) en la gestión y procesamiento de información. En la actualidad, la IA constituye una herramienta esencial para la optimización de procesos en múltiples sectores; no obstante, su aplicación genera desafíos complejos relacionados con la privacidad, seguridad, transparencia, rendición de cuentas y responsabilidad jurídica. La ausencia de una regulación específica que contemple estos aspectos puede conllevar a la vulneración de los derechos de los titulares de datos y al uso desproporcionado o inadecuado de tecnologías automatizadas sin los debidos mecanismos de supervisión. El estudio realiza un análisis crítico del desarrollo normativo ecuatoriano en protección de datos, contrastándolo con estándares internacionales y modelos regulatorios implementados en otras jurisdicciones. Además, incorpora principios orientadores aún no normativizados, pero fundamentales para la construcción de un marco legal robusto. A partir de este análisis, se propone una reforma legislativa que garantice un equilibrio entre la innovación tecnológica y la tutela de los derechos fundamentales, mediante la creación de instrumentos legales que permitan el monitoreo, la auditoría y el control ético y responsable del uso de la IA.

Palabras clave: *Inteligencia artificial, protección de datos, regulación.*

ABSTRACT

This research examines the urgent need to reform the Ecuadorian legal framework on personal data protection, aiming to effectively integrate the use and control of artificial intelligence (AI) in information management and processing. Currently, AI is an essential tool for optimizing processes across multiple sectors; however, its application presents complex challenges related to privacy, security, transparency, accountability, and legal responsibility. The lack of specific regulations that address these issues can result in violations of data subjects' rights and the disproportionate or improper use of automated technologies without adequate oversight mechanisms. The study presents a critical analysis of Ecuadorian regulatory developments in data protection, contrasting them with international standards and regulatory models implemented in other jurisdictions. Furthermore, it incorporates guiding principles that, while not yet codified, are fundamental to building a robust legal framework. Based on this analysis, a legislative reform is proposed to ensure a balance between technological innovation and the protection of fundamental rights through the creation of legal instruments that enable monitoring, auditing, and the ethical and accountable use of AI.

Keywords: *Artificial intelligence, data protection, regulation.*

INDICE

INTRODUCCIÓN

La rápida evolución de la inteligencia artificial ha transformado diversos sectores potenciales sobre la eficacia y la innovación. Sin embargo, este avance tecnológico plantea desafíos significativos en materia de protección de datos personales, especialmente en países como Ecuador, donde la narrativa vigente aún no aborda de manera específica a estas nuevas realidades. En 2021, Ecuador promulgó la ley orgánica de protección de datos, con el objetivo de salvaguardar la privacidad de los ciudadanos y regular el tratamiento de su información personal. No obstante, esta ley no contempla de forma explícita las implicaciones de la guía en el manejo de datos, lo que genera vacíos legales que podrían ser explotados en cuánto a los derechos de los individuos que se encuentran sin un cierto manejo de sus derechos debido a que no existe por el momento algún tipo de ley la cual sea de carácter estricto irregular a la inteligencia artificial conforme a la voluntad y a su consentimiento en cuanto al método el cual aplica un cierto tipo de control sobre el individuo debido a que se acepta de una forma explícita e involuntaria en algunos casos un cierto tipo de conocimiento por ha sido siglo el cual genera una especie de contrato entre una tecnología conocida como la inteligencia artificial y el individuo, pero este contrato por así decirlo no se les establecen cláusulas ni normativas para llegar a regularizar su control es por ello que debería introducirse un cierto tipo de control o de ley que promueva una limitante para la inteligencia artificial.

A nivel internacional, la unión europea ha implementado el reglamento general de protección de datos, que establece un Marco robusto para la protección de datos personales, incluyendo disposiciones sobre la toma de decisiones automatizadas y la transparencia en el proceso o procesamiento de datos. Este reglamento ha servido de referencia para muchas jurisdicciones en la elaboración de sus propias normativas de protección de datos.

La ausencia de una regulación específica sobre IA en la LOPDP plantea la necesidad de crear o modificar la normativa existente para incluir disposiciones que aborden estos desafíos. Esta regulación debería establecer límites claros en el uso de algoritmos, decisiones automatizadas y procesamiento masivo de información, garantizando la transparencia, la rendición de cuentas y la seguridad en el uso de la IA. Además, la creciente tendencia global hacia una mayor regulación de

las plataformas digitales y el uso de tecnologías avanzadas, como la IA, resalta la importancia de que Ecuador adapte su marco legal para alinearse con estos estándares internacionales y proteger eficazmente los derechos de sus ciudadanos. (Luis Enrique Velasco, 2024)

La inteligencia artificial representa tanto una oportunidad como un desafío para la protección de datos personales debido a que su uso es cotidiano y reciente debido a que se han implementado nuevas tecnologías dentro de los navegadores y aplicaciones los cuales todavía no tienen un modus operandi debido a la falta de regularización dentro del Estado. Su uso masivo en la recolección, análisis y procesamiento de información exige una regulación clara y efectiva que garantice el equilibrio entre la innovación y el respeto a los derechos fundamentales. Ecuador enfrenta una brecha normativa que podría derivar en vulnerabilidad de privacidad, discriminación Algorítmica y la falta de transparencia en la toma de decisiones automatizadas, puesto que estas tecnologías utilizan un modus operandi el cual es completamente automatizado y graban dentro de su nube cierta información la cual en algún punto puede llegar a ser robada , esto debido a que personas expertas en la tecnología pueden llegar a buscar la manera de vulnerar los sistemas tecnológicos y adentrarse dentro de las bases de datos las mismas que pueden tener información de carácter privado. Dentro del tema de la inteligencia artificial se ha visto un comportamiento completamente automatizado el cual como mencionamos anteriormente puede vulnerar el derecho de las personas se hace necesario examinar como la información almacenada en nubes digitales y utilizada por algoritmos podría ser explotada sin el consentimiento adecuado de los usuarios.

Muchas personas aceptan términos y condiciones sin comprender plenamente el alcance del uso de sus datos personales, lo que lleva a situaciones en las que su privacidad puede ser comprometida sin su consentimiento. En este sentido, es fundamental que las futuras reformas incluyen mecanismos de información y educación digital Que permitan a los ciudadanos tomar decisiones informadas sobre su privacidad y la gestión de sus datos, esto es un impulso para la ciudadanía ya que muchas de las veces al descargar una nueva aplicación aceptamos los términos y condiciones si ni siquiera saber lo que estamos aceptando, esto puede generar cierto tipo de riesgo ya que podemos Aceptar que utilicen información de carácter privada que tenemos dentro de nuestro móvil o computadora y utilizarla a su favor.

La inteligencia artificial ha emergido como una de las tecnologías más disruptivas del siglo XXI, transformando la manera en que se procesan y gestionen grandes volúmenes de datos. Sin embargo, este avance ha generado importantes desafíos en términos de protección de datos

personales, especialmente en países como Ecuador, donde la legislación en materia de privacidad y protección de datos aún no se ha adaptado completamente a las nuevas realidades tecnológicas cómo es las tecnologías que utilizan la IA. La Ley Orgánica de Protección de Datos Personales, promulgada en 2021, establece principios fundamentales para la protección de la privacidad, pero presenta limitaciones significativas frente a los avances de la IA y el tratamiento automatizado de datos debido a que esta tecnología es reciente y todavía no se ha explorado por completo lo que se puede llegar a desprender de la misma.

Dentro de nuestra investigación se abordan distintos aspectos relacionados con la protección de datos personales en Ecuador en el contexto desarrollado y el uso de la IA. Es por ello que existen capítulos los cuales entran en la Ley Orgánica de Protección de Datos Personales, sus alcances y limitaciones, Analizando las áreas en las que la ley es insuficiente frente a los rápidos de avances tecnológicos. También se exploran la falta de regulación específica sobre IA, los riesgos asociados a la gestión de datos sin normativas claras y los desafíos que enfrenta Ecuador en su aplicación efectiva.

También se examinará a las normativas internacionales más relevantes, como el reglamento general de protección de datos de la Unión Europea, y como estas regulaciones abordan el uso de IA en la protección de datos. A través de ejemplos como son los países de España, Alemania, Canadá y Brasil, se identificarán ciertos modelos preventivos y enfoques que podrían servir como referencia para nuestro país, destacando las diferencias que existen entre sus leyes y la ley orgánica de protección de datos personales la cual se encuentra regularizada dentro de nuestro país y a su vez veremos y analizaremos los vacíos normativos que limitan la adopción de estas mejores prácticas

Nos ha adentraremos en los riesgos éticos derivados del uso de la IA en el tratamiento de datos personales. Se discutirán problemas como el sesgo algorítmico, la opacidad en los sistemas de IA y los desafíos legales relacionados con la responsabilidad en el uso de estas tecnologías. Se propondrán estrategias para mitigar estos riesgos y asegurar un uso ético de la IA, considerando también el papel de la educación digital en la protección de los derechos de los ciudadanos.

Existirá un enfoque en la necesidad urgente de una reforma legal que regule de manera integral la IA en Ecuador. Se explorarán los principios clave que deben guiar esta reforma, la creación de un ente supervisor independiente y la implementación de mecanismos de auditoría y transparencia en los sistemas de IA. Además, se propondrán modificaciones específicas a la Ley

Orgánica de Protección de Datos Personales para garantizar que la legislación ecuatoriana esté alineada con las mejores prácticas internacionales, sin comprometer la innovación tecnológica.

Dentro de la investigación e indagación que vamos a realizar buscando distintos puntos de controversia y conflicto, esta tesis busca contribuir al desarrollo de un Marco legal que proteja de manera efectiva a los derechos de los ciudadanos en un entorno digital cada vez más complejo. Se pretende asegurar que el avance de la inteligencia artificial no ponga en riesgo a la privacidad y seguridad de los datos personales, en un contexto donde distintas plataformas interactúan de forma automatizada y almacenan información personal en la nube sin garantizar siempre la debida protección y transparencia en su uso.

Capítulo 1: Protección de datos en Ecuador y desafíos ante la IA

1.1 LOPDP: Alcance y limitaciones

Dentro de la Ley Orgánica de Protección de Datos Personales se establece una norma estricta y vigente para que no exista una vulneración de derechos sobre datos personales esto actúa de forma general para el Estado, es así que estas leyes se limitan acciones que pueden generar una problemática, pero con el avance de la tecnología y varios dispositivos o aplicaciones se ha generado cierta controversia sobre lo que se puede llegar a realizar sin que exista un perjuicio hacia otra parte, que quiero decir con esto, pues que dentro de nuestro nuevo mundo, un mundo enfocado en el avance tecnológico y nuevas tecnologías y métodos que usan sistemas automatizados, se guarda mucha información dentro de una nube o una de base de datos la misma que establece ciertos aspectos que implican confidencialidad que puede llegar a ser vulnerada, se crean nuevos enfoques los cuales no regularizan o establece una limitante general sobre hasta donde se puede llegar a obtener información personal o hasta donde se puede establecer el carácter de confidencialidad, esto se podría llegar a entender como una cierta clase de contrato entre una máquina y un individuo debido a que se acepta términos y condiciones para el uso de la aplicación o de la página, sin tener un conocimiento previo de cuanto información personal puede usar, debido a que no se pacto una limitante a la intimidad, es por eso que se debería buscar un respaldo, el cual cuente con una base solida que proteja la información de carácter personal de una forma segura.

> En Ecuador, el entorno digital en crecimiento exige marcos claros para proteger los derechos de los usuarios. La Ley Orgánica de Protección de Datos Personales (LOPDP), aprobada en 2021, es un instrumento clave para garantizar el uso responsable de la información, alineando al país con estándares internacionales y fomentando la confianza en la economía digital. Sin embargo, su implementación enfrenta desafíos, como la falta de claridad en su aplicación para empresas e instituciones, y la necesidad de que los ciudadanos comprendan mejor sus derechos y responsabilidades respecto a la protección de datos. (Rodríguez Almache, 2024)

Desde mi perspectiva es fundamental comprender que la ley orgánica de protección de datos personales para poder analizar de una manera crítica sus alcances y limitaciones en el contexto actual, especialmente en Ecuador, donde la regulación de la inteligencia artificial aún no está plenamente integrada en el Marco normativo de protección de datos. Aunque la Ley Orgánica de Protección de Datos Personales es un avance importante en la salvaguarda de la privacidad y los derechos digitales de los ciudadanos, su promulgación en 2021 no contempló de manera específica los retos que plantea la IA en el tratamiento personal de datos debido a que de cierta manera no existe un capítulo o normas las cuales específicamente traten sobre bases de datos o almacenamiento de información de datos que sean de carácter automatizado o a su vez que respondan a un sistema de logaritmo los cuales tengan un carácter automático.

En Ecuador, como en muchos otros países de la región, la conciencia sobre la protección de datos aún es limitada. Muchas personas aceptan términos y condiciones sin leerlos, proporcionando información personal simple a comprensión de cómo será utilizada o a su vez de dónde será guardada o almacenada. En este sentido, la Ley Orgánica de Protección de Datos Personales establece principios esenciales como la solicitud, la lealtad, la transparencia y la minimización de los datos, pero la realidad es que sin una supervisión eficaz y sin mecanismos de aplicación claros, estos principios pueden quedarse en simples formalidades.

Uno de los principales problemas es la falta de un marco regulador que aborde de manera específica el uso de la IA en el tratamiento de datos personales. La IA tiene la capacidad de procesar grandes volúmenes de información en segundos y asimismo tomar decisiones

automatizadas y generar perfiles detallados de las personas sin que estas sean plenamente conscientes de ellos, Esto lo hace de forma automática ya que su base de conocimiento y sus volúmenes de datos que tiene es literalmente todo lo que se puede encontrar en la web. Esto puede dar lugar a riesgos como la discriminación algorítmica, la recopilación de datos sin consentimiento explícito y la falta de transparencia en la toma de decisiones. En Ecuador, donde aún se está fortaleciendo la cultura de protección de datos, la ausencia de una regulación específica sobre IA podría facilitar prácticas que vulneren la privacidad de los ciudadanos de su información personal.

Es necesario que la Ley Orgánica de Protección de Datos Personales sea reformada, para que se establezcan nuevas directrices claras y completas sobre el uso de la IA en la gestión de datos personales. Una de las medidas fundamentales, y una de las bases las cuales se debería identificar es garantizar una transparencia en los algoritmos y la toma de las decisiones que son de carácter individualizado y a su vez automático. Las empresas y entidades gubernamentales que utilicen la IA para procesar datos personales deberán ser obligadas a informar de manera clara cómo funciona sus algoritmos y a su vez qué información se le puede indicar y dar a esto cierto tipo de tecnologías, que criterios utilizan y qué impacto pueden tener en los derechos de las personas.

Otra de las medidas clave es el consentimiento informado y la protección del usuario. Actualmente, en muchas de las plataformas que obtienen datos de los usuarios no existe un conocimiento real de cómo son utilizadas y de cómo se llega a ese cierto tipo de consentimiento. Se debe establecer normativas que garanticen que el consentimiento sea verdaderamente informado y que las personas tengan la opción de rechazar dicho tratamiento de datos sin perder el acceso a servicios esenciales ya que no debería ser una obligación aceptar un consentimiento el cual permita utilizar otras aplicaciones las cuales puedan contener cierta información de carácter privado para utilizar una aplicación que nada tenga que ver con su privacidad, es así que debería utilizarse un consentimiento informado y detallado sobre qué es lo que se va a establecer y qué es lo que se va a tratar, y no se debe obligar a aceptar términos y condiciones para el uso de las aplicaciones, esto sin relación a un principio de transparencia, puesto que los términos y condiciones son manifestados, sin embargo la obligación de aceptar estos términos para poder usarla debería ser nulo.

Además, es indispensable contar con una supervisión y una auditoría de los sistemas de IA. Ecuador necesita un ente regulador especializado en inteligencia artificial y a su vez especializado en la protección de datos que se encargue de auditar los sistemas de inteligencia artificial que

manejen información personal y garanticen que su funcionamiento se ajuste a los principios de la Ley Orgánica de Protección de Datos Personales cuando la misma tenga una regulación más estricta sobre las nuevas tecnologías que aborda nuestro país. Sin embargo, sin la existencia de un mecanismo de supervisión adecuado, el uso de la inteligencia artificial en la gestión de datos podría derivar en prácticas abusivas o discriminatorias las cuales no pueden llegar a ser controladas o no se puede llegar a generar un cierto grado de limitante hacia algunas tecnologías.

De igual manera la implementación de sanciones efectivas es una pieza fundamental dentro de una regulación, la legislación debe complementar sanciones proporcionales y efectivas para aquellas empresas y entidades que cumplan las disposiciones de la Ley Orgánica de Protección de Datos Personales en relación con el uso de la inteligencia artificial, Esto es como una base la cual puede llegar a limitar sobre el accionar de empresas o entidades que abusen de la inteligencia artificial, al haber una sanción de por medio va a generar miedo y control para que no exista este abuso. Si un mecanismo de control estricto la normativa pierde fuerza y deja expuestos a los ciudadanos frente a posibles vulneraciones de privacidad y de derechos digitales.

Finalmente, la educación digital y la conciencia ciudadana son elementos fundamentales para la efectividad de cualquier tipo de regulación. Es imprescindible que los ciudadanos conozcan sus derechos en materia de protección de datos y sepan cómo ejercerlos de una manera la cual no engañe o vulnere los derechos que debemos tener. Para ello, se deben impulsar campañas de educación digital que permitan comprender la importancia de la privacidad en esta era digital y la forma en que la inteligencia actual puede influir en sus vidas y a su vez vulnerar algún cierto tipo o grado de relación entre una inteligencia automatizada y un ciudadano. Sólo a través de un cuerpo normativo sólido, con mecanismos de supervisión adecuados y una ciudadanía informada, se podrá garantizar un uso responsable ético y formal de una inteligencia artificial en Ecuador.

Nuestro país tiene la oportunidad de fortalecer su legislación en materia de protección de datos personales, tomando en cuenta los avances tecnológicos y los desafíos que plantea la inteligencia artificial y su rápido proceso y avance al sacar cada año o cada mes o cada día una nueva tecnología la cual es aún más humana. La Unión Europea, con su reglamento general de protección de datos, ha establecido un marco regulador que podría servir como una referencia o una base para nuestro país. Adoptar ciertos principios de forma similar y adoptarlos a nuestra realidad ecuatoriana permiten garantizar una innovación tecnológica sin que exista o sin que se convierta en una amenaza para los derechos fundamentales de nuestros ciudadanos, en conclusión,

la Ley Orgánica de Protección de Datos Personales es un pilar clave para la protección de privacidad en Ecuador, pero requiere de algunos tipos de actualizaciones urgentes para hacer frente a los desafíos que plantea la inteligencia artificial. La transparencia, la supervisión efectiva y la educación ciudadana como se mencionó anteriormente son elementos esenciales que deben ser incorporados dentro de la legislación ecuatoriana Para garantizar un equilibrio entre el avance tecnológico y la protección de los derechos de los ciudadanos un control es como un cierto tipo de ayuda y de base para que no exista un descontrol ciudadano.

1.1.1. Principios y objetivos de la LOPDP

En Ecuador principalmente el Estado se rige por varios principios y objetivos que son primordiales para establecer un control y una limitante para el pueblo, es por ello que para la mayoría de ámbitos se establecen principios que son pilares para establecer un control, en la Ley Orgánica de Protección de Datos Personales se establecen varios principios que son base para un control y una seguridad social, mismos que serán estudiados y analizados para llegar a comprender y tener más énfasis sobre cómo se puede llegar a obtener una limitante para ciertas tecnologías las cuales pueden llegar a tener un abuso debido a que no existe una legislación que les ponga un control.

Consentimiento

> Art. 8.-Consentimiento. -Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea: 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento; 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento; 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia, 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular. El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un

> procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos. (Ley Orgánica de Protección de Datos Personales, 2021, pág. articulo 8)

El principio del consentimiento en la Ley Orgánica de Protección de Datos Personales del Ecuador representa un avance significativo en cuanto a la autonomía y derechos de los individuos sobre su propia información. Sin embargo, la práctica para obtener un consentimiento claro, libre e informado, plantea ciertos desafíos, ya que no existe un ente que regule la transparencia y la seguridad de las bases de datos, mismas bases que almacenan la información personal. Las organizaciones deben asegurarse de qué el consentimiento no sea sólo un requisito formal, sino una opción libre y voluntaria para los titulares de los datos. Además, el hecho de que el consentimiento puede ser revocado en cualquier momento introduce un mecanismo de control adicional para los usuarios, pero también exige a las empresas una infraestructura que permita modificar y gestionar rápidamente el tratamiento de los datos en caso de Retiro del consentimiento, lo cual puede generar dificultades operativas. Por una parte está bien que las empresas deban informar a las personas de manera clara y comprensible sobre cómo se utilizarán los datos personales Debido a que esto menciona un cierto grado de ética sobre la empresa y consumidor ya que esto se debería tomar dentro de todo tema puesto a que dentro de una inteligencia artificial no existe el mismo ya que este toma decisiones automatizadas muchas de las decisiones no están controladas por un individuo es por ello que muchas de las decisiones son de carácter incomprensible ya que una máquina no puede sentir o no puede razonar de una forma en la cual una persona o un ser humano lo haría.

Finalidad

> Art. 1.-Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (Ley Orgánica de Protección de Datos Personales, 2021, pág. ART.1)

Este principio establece que los datos personales deben ser recolectados y utilizados solo para fines específicos, legítimos y claramente informados, esto busca evitar el uso indiscriminado de la información ya que muchas de las veces no existen un control basto sobre la información que se brinda y lo que puede llegar a ser utilizado por algún cierto tipo de persona, entidad o empresa. No obstante, el verdadero reto se presenta cuando las empresas requieren adaptarse a cambios imprevistos en el mercado o en alguna de sus operaciones las cuales ya tenían un modo de operación, esto debido a que puede generar la necesidad de utilizar los datos personales para fines distintos a lo que inicialmente fueron establecidos, ahí ya existe una disrupción de lo que se debe tomar o de lo que se haya establecido anteriormente ya que con el principio, la finalidad de los datos se encuentran claramente establecidos con un propósito y al momento en el cual existe una disrupción, lo que fue dispuesto, se estaría vulnerando los derechos de la persona. En estos casos, el principio de finalidad establece una limitante sobre la protección del individuo, pero también podría limitar la flexibilidad de las organizaciones al dificultar la adaptabilidad de su tratamiento de datos sin un consentimiento adicional, esto resalta la estrecha tensión que existe entre la protección de los derechos de los individuos y las necesidades que puede llegar a presentar una empresa en el manejo de la información de manera eficiente.

Calidad de datos

Calidad y exactitud. -Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales. Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos: a) Hubiesen sido obtenidos por el responsable directamente del titular.

> b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable. c) Fuesen obtenidos de un registro público por el responsable. (Ley Orgánica de Protección de Datos Personales, 2021, pág. ART. 10)

La calidad de datos es esencialmente para que las decisiones basadas en ellos sean precisas y confiables, esto genera un cierto tipo de relación que pone o genera una comprensión sobre lo que se va a tener en cuenta y lo que va a ser utilizado. Sin embargo, Este principio coloca una carga significativa sobre las empresas para garantizar la exactitud y la actualización constante de los datos personales que se poseen. Ciertas organizaciones deben implementar sistemas que permiten la corrección de datos erróneos y asegurar que la información delimitada en realidad sea de los titulares de los datos. Este principio también plantea la cuestión de la cantidad de recursos que las empresas deben invertir en la verificación y mantenimiento de la calidad de los datos, especialmente en contextos de alta rotación de información o sectores donde los datos cambien con frecuencia.

Proporcionalidad

La proporcionalidad es uno de los principios fundamentales en la Ley de Protección de Datos en Ecuador. Este principio establece que la recolección y tratamiento de datos personales debe ser acorde y proporcional a la finalidad para la cual se recopilan. Esto significa que las organizaciones deben recopilar únicamente los datos personales necesarios y pertinentes para cumplir con la finalidad establecida. No se permite la recolección excesiva o innecesaria de datos que exceda el propósito original. Además, el principio de proporcionalidad también implica que el tratamiento de los datos debe ser realizado de manera adecuada y proporcionada, utilizando las medidas técnicas y

organizativas necesarias para garantizar la seguridad y confidencialidad de la información. (Ley Orgánica de Protección de Datos Personales, 2021, pág. ART10)

El principio de proporcionalidad se asegura de que se recopile los datos estrictamente necesarios para alcanzar la finalidad establecida. Si bien este principio busca prevenir la invasión innecesaria de la privacidad, su implementación práctica puede ser compleja, ya que no siempre es fácil determinar qué información es estrictamente necesaria para un propósito específico. Esto debido a que no tenemos un conocimiento completamente adaptado sobre lo que se puede llegar a necesitar para llegar a generar una acción. Además, las empresas deben encontrar un equilibrio entre la obtención de la cantidad de datos suficientes para su objetivos y el respeto a la privacidad de los individuos, esto por el momento no se puede controlar de una forma general debido a que no existe la legislación que vincule a la privacidad con los datos personales o no existe una limitante de que es, o hacia donde se puede dirigir una base de datos que cuente, o sea conformada por toda la información, la cual haya sido establecida mediante algún mecanismo automatizado que involucre ciertos tipos de algoritmos que se puedan establecer para la obtención de una base de datos de carácter personal. En algunos casos, las organizaciones podrían sentirse limitadas por este principio al no poder acceder a datos adicionales que podría mejorar la calidad de sus servicios o análisis esto con el miedo de que exista una vulneración de un derecho de privacidad de una persona ya que al no tener una regulación se puede llegar a comprometer la misma.

Seguridad

La seguridad de los datos personales es un aspecto crucial dentro de la Ley de Protección de Datos en Ecuador. Esta ley establece que las organizaciones deben implementar medidas de seguridad adecuadas para proteger la información personal de accesos no autorizados, pérdidas o daños. Estas medidas de seguridad pueden incluir el uso de tecnologías de encriptación, contraseñas seguras, firewalls, sistemas de detección de intrusos, entre otros. Además, las organizaciones deben establecer políticas internas y procedimientos para garantizar la adecuada protección de los datos personales. Es importante destacar que la seguridad de los datos no solo se refiere a la protección de los

> datos almacenados en sistemas informáticos, sino también a su manipulación, transmisión y almacenamiento físico. Esto implica que las organizaciones deben contar con medidas de seguridad tanto tecnológicas como físicas. (Ley Orgánica de Protección de Datos Personales, 2021, pág. ART10)

La seguridad de los datos personales es uno de los principios bases y fundamentales para evitar el acceso no autorizado, la pérdida o el daño de la información, o a su vez una vulneración de un derecho de una persona. A pesar de que la ley exige medidas adecuadas de seguridad, su implementación efectiva puede resultar costosa y técnicamente desafiante, especialmente para pequeñas y medianas empresas que no cuenten con una base sólida. Además, la protección de datos no sólo debe centrarse en las herramientas tecnológicas, sino también en los procesos internos, como la capacitación del personal y la creación de protocolos para manejar incidentes de seguridad. En un mundo cada vez más digital y una era cada vez más tecnológica una de las bases en las cuales se debe asentar no sólo el estado sino el mundo entero es sobre la seguridad de los datos personales y hasta donde se puede llegar a vulnerar la privacidad de una persona comprendiendo así un tema en el cual no se tiene un contexto estricto de lo que es la intimidad y de lo que es la privacidad de la persona.

1.1.2. ¿Quiénes están protegidos por la LOPDP?

Dentro de la ley orgánica de protección de datos personales pueden existir dos tipos de personas a las cuales se les puede vulnerar los derechos, es por ello que dentro de la ley esta va dirigida y hace un análisis tanto para las personas naturales como para las personas jurídicas, es por ello que cada uno de estos temas se va a profundizar y analizar de una forma secuencial.

Personas naturales

> Las personas naturales, es decir, los individuos que tienen derechos y obligaciones, están amparadas por la Ley de Protección de Datos en Ecuador. Esto significa que cualquier información personal que sea recopilada, almacenada o utilizada por terceros debe ser tratada de acuerdo con los principios y disposiciones establecidos en la ley. La ley establece

> que las personas naturales tienen el derecho de conocer qué información se está recopilando sobre ellas, así como el propósito para el cual se está utilizando. Además, tienen el derecho de acceder a sus datos personales, corregir cualquier información incorrecta y solicitar la eliminación de sus datos de las bases de datos de las organizaciones que los almacenan. Además de estos derechos, las personas naturales también tienen la posibilidad de presentar denuncias ante la Agencia de Protección de Datos Personales en caso de que consideren que sus derechos han sido vulnerados. Esta entidad se encarga de investigar y sancionar cualquier infracción a la ley en materia de protección de datos personales**.** (DATOS PERSONALES PROTEGIDOS, 2022)

Las personas naturales las cuales son entendidas como individuos que gozan de derechos y obligaciones que lo comprende un marco jurídico son las que se encuentran protegidas por la ley, esta ley establece un conjunto de normativas y principios que están fríamente diseñados para garantizar el tratamiento adecuado de la información personal de los ciudadanos sin que se dé una vulneración de los derechos de las mismas personas. De acuerdo con la legislación ecuatoriana, cualquier recopilación o almacenamiento de datos personales deben cumplir con ciertas disposiciones que aseguran una protección y un respeto de los derechos fundamentales de las personas, en este caso sería la no vulneración de los derechos de intimidad y privacidad.

En este contexto, se reconocen algunos derechos de forma específica para las personas consideradas naturales en relación con sus datos personales e información personal. Entre estos derechos se destaca el derecho a la información, el cual permite conocer qué datos están recolectando sobre ellos y a su vez cuál es la finalidad de tener esta información; el derecho a la corrección, este es el que faculta a los individuos a rectificar cualquier cierto defecto o error que haya sido puesto a lo mejor por un error de tipeo o a su vez por una confusión; y el derecho de supresión, que les permite solicitar la eliminación de sus datos de la base de datos debido a que no se autorizó o a su vez ya no encuentra necesario que esa información se encuentre dentro de lo que son las bases de datos y asimismo se gestiona para que se borren de forma inmediata esta información.

Adicionalmente, las personas naturales tienen a su disposición ciertos tipos de mecanismos a favor de la protección ante el hecho de que pueda existir posibles violaciones a sus derechos en materia de datos personales. La ley establece que, en caso de considerar que sus derechos han sido vulnerados o están al borde de ser vulnerados, los individuos pueden presentar denuncias ante la superintendencia de protección de datos personales, la cual por obligación tiene que cumplir y salvaguardar a la persona y a su información privada la cual está haciendo vulnerada o está al borde de ser vulnerada. Esta intendencia como mencioné anteriormente tiene una responsabilidad a su vez de investigar los casos presentados y sancionar si es que existe algún tipo de infracción la cual vaya contra la ley, esto con el fin de garantizar un cumplimiento de la normativa y la protección efectiva de los derechos de los ciudadanos.

De esta manera, la Ley Orgánica de Protección de Datos Personales en el Ecuador refuerza el concepto de autonomía y control de las personas naturales sobre su propia información, promoviendo lo que sería la transparencia, la seguridad y la confianza en el manejo de los datos personales y privados.

Personas jurídicas

Las personas jurídicas, como las empresas, también están protegidas por la Ley de Protección de Datos en Ecuador. Aunque la ley se enfoca principalmente en la protección de los datos personales de las personas naturales, también establece ciertas obligaciones para las organizaciones en relación con el tratamiento de los datos de las personas jurídicas. En este sentido, las empresas deben garantizar la confidencialidad y seguridad de los datos que recopilan y utilizan en el desarrollo de sus actividades. Además, deben obtener el consentimiento de las personas jurídicas antes de utilizar sus datos para fines distintos de aquellos para los que fueron recopilados inicialmente. La Ley de Protección de Datos en Ecuador también establece que las personas jurídicas tienen el derecho de acceder a la información que se encuentra en poder de otras organizaciones, así como el derecho de

> rectificar cualquier información incorrecta o solicitar la eliminación de sus datos de las bases de datos de terceros. (DATOS PERSONALES PROTEGIDOS, 2022)

Este articulo nos menciona que las personas jurídicas, como las empresas u organizaciones, también están sujetos a las disposiciones de la ley orgánica de protección de datos en el Ecuador. No obstante, las entidades jurídicas deben cumplir con una serie de obligaciones en relación con el tratamiento de los datos los cuales ellos almacenan y generan dentro de una base de datos, tanto de sus empleados como de sus clientes u otros interesados.

La legislación ecuatoriana establece que todas las personas jurídicas tienen una responsabilidad, esta responsabilidad es la de garantizar la seguridad y confidencialidad de las personas de las cuales se recopilan sus datos, ya que estos datos son almacenados y procesados en el curso de sus actividades comerciales o empresariales, esto dependiendo a qué se dedique cada una de las empresas. Esto implica implementar medidas adecuadas para la protección de la información contra algún tipo de acceso no autorizado, pérdidas o alteraciones indebidas, o a su vez un hackeo de datos. Además, las organizaciones deben obtener el consentimiento explícito de las personas jurídicas cuando vayan a utilizar sus datos para finalidades diferentes aquellas para las que fueron inicialmente recolectados, esto con el fin de precautelar una relación sana y a su vez consentida sobre el ¿Para qué? del uso de sus datos personales.

Asimismo, la Ley Orgánica de Protección de Datos Personales en Ecuador reconoce algunos derechos para las personas jurídicas. Entre estos derechos se incluye la posibilidad de acceder a los datos de otras organizaciones, esto con el fin de verificar su exactitud y asegura que no existan inconsistencias o algún tipo de cambio dentro de los datos y que sean estos de carácter seguro y verificables. En caso de qué esta información se encuentre alterada o se encuentre incorrecta, las personas jurídicas tienen el derecho de solicitar la corrección de la misma. Igualmente, pueden solicitar la eliminación de sus datos de la base de datos de terceros, siempre que este no contravenga otras normativas o compromisos legales que se encuentren dispuestos dentro del ordenamiento. Finalmente podemos demostrar que la Ley Orgánica de Protección de Datos Personales en Ecuador, se enfoca principalmente en la protección de datos personales de las personas naturales. También establece algunos aspectos que son muy importantes para las personas jurídicas, esto con el fin de promover la transparencia y el control social, debido a que, si es que

no existe un control, se puede llegar a la vulneración de los derechos de las personas esto tanto para las personas naturales como para las personas jurídicas.

1.1.3. ¿Qué problemas presenta frente a los avances tecnológicos?

Debido a los avances tecnológicos que han transformado a nuestra vida cotidiana, surgen cuestionamiento sobre los límites de la confidencialidad, la privacidad y la intimidad de las personas. En este contexto, se han desarrollado diversos criterios que generan preocupaciones sobre el impacto de las nuevas tecnologías y su constante evolución. Un aspecto relevante es el uso de aplicaciones con funciones automatizadas, las cuales interactúan con los usuarios sin intervención humana directa. Estas aplicaciones, mediante algoritmos avanzados, pueden generar respuestas sin necesidad de una orden explícita la cual sea mandada por un humano, lo que genera inquietudes respecto a su inteligencia, capacidad de recuperación de datos y la forma que gestiona la información personal de los usuarios.

Uno de los hábitos más comunes en la actualidad es aceptar los términos y condiciones de una aplicación sin leerlos detenidamente. Al instalar o acceder a una plataforma digital nosotros aceptamos lo que son los términos y condiciones y a su vez aceptamos un compromiso con la aplicación de qué ella pueda llegar a utilizar nuestra información privada o utilizar ciertas aplicaciones que pueden ser de carácter personal, dentro de la aceptación de los términos y condiciones muchas de las veces se acepta utilizar la cámara, galería, micrófono, etc. Es por ello que debemos fomentar la lectura antes de aceptar cualquier tipo de término o condición que brinde alguna aplicación determinada, dentro de nuestra legislación no existe todavía normas las cuales regulan este aspecto es por ello que no se sabe con exactitud algún tipo de sanción que se pueda establecer por una violación de derechos, por ejemplo.

En el marco de las nuevas tecnologías, la inteligencia artificial ha adquirido un papel protagónico, ofreciendo respuestas automatizadas y personalizadas basadas en la información proporcionada por los usuarios. Sin embargo, esta capacidad plantea desafíos significativos en materia de protección de datos. La guía puede almacenar información en servidores de la nube, lo que genera incertidumbre sobre su seguridad y el posible uso indebido de los datos recopilados. Además, existe el riesgo de que los delincuentes cibernéticos accedan a bases de datos donde se encuentra información privada, misma que lleguen a utilizar mediante algún tipo de aplicación para robar esta información que es de carácter privado, personal e íntimo. La falta de transparencia

en la gestión de la información por parte de muchas plataformas que emplean inteligencia artificial refuerza la necesidad de establecer regulaciones claras que garantiza la protección de los datos personales.

Actualmente, es común que las personas se comuniquen con la inteligencia artificial como si trataran de un interlocutor humano, confiando en ella como si fuera un amigo, médico, psicólogo o consejero. Dado que la inteligencia artificial responde con precisión y rapidez a las diversas inquietudes, los usuarios pueden compartir información personal y confidencial sin considerar las implicaciones de seguridad. Esta información queda almacenada en la base de datos y en la nube la cual la aplicación lo tiene por defecto. Esta información como mencionamos que, almacenada en esta base de datos, que, en muchos casos, son utilizadas para mejorar los sistemas de inteligencia artificial mediante el aprendizaje automático. No obstante, persiste la incertidumbre sobre el nivel de protección de esta base de datos y el riesgo de qué personas con conocimientos cibernéticos o tecnológicos accedan a ellos con fines ilícitos. Entre los posibles delitos que pueden derivarse del uso indebido de la inteligencia artificial se encuentra el robo de la identidad, la extorsión y el acceso a información personal.

Ante estas preocupaciones surge la interrogante sobre la necesidad de establecer normativas específicas que regulan un desarrollo y un uso de la inteligencia artificial. Dado que esta tecnología aún es relativamente nueva, es fundamental llevar a cabo investigaciones más profundas para comprender su funcionamiento, sus implicaciones éticas y su impacto en la privacidad. La implementación de regulaciones adecuadas permitirá un uso más seguro y transparente de la inteligencia artificial, garantizando que el avance tecnológico no compromete a los derechos fundamentales que tienen las personas desde que llegan a nacer.

Este también considero yo que es un desafío ético debido a que las personas que utilizan estas inteligencias deben priorizar la moralidad puesto que estas tecnologías deben estar para expandir el conocimiento, el aprendizaje, y la enseñanza más que llegar a vulnerar los derechos o buscar intimidar, robar, extorsionar a las personas.

1.2. Falta de regulación sobre IA

1.2.1. ¿Por qué la LOPDP no menciona explícitamente la IA?

Dentro de los ordenamientos que establece la Ley Orgánica de Protección de Datos Personales, no se generaliza o se identifica una norma la cual vincule de forma directa a la inteligencia artificial, sin embargo, se puede llegar a vincular con cientos de artículos como pueden ser:

"Art. 8.-Consentimiento. -Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea: 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento; 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento; 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia, 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular. El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos." (LOPDP, 2022, pág. ART 8)

Aquí podemos observar que se hace mención a un consentimiento que puede considerarse como una práctica tradicional entre el usuario y la aplicación, en la cual se expresa un consentimiento por parte del usuario, otorgando una cierta responsabilidad o más bien un poder para realizar diversas actividades en nombre del mismo. Esto se podría identificar como una especie de contrato el cual se da entre el consumidor y la aplicación por así decirlo que medianamente se podría entender a la aplicación como un jefe, ya que él va a tener control sobre nosotros, en lugar que nosotros sobre él. Esto implica que no existe un límite claro sobre la cantidad de información que se puede proporcionar, lo que deja al usuario en una posición donde, al otorgar este consentimiento, abre la puerta para que su información personal sea manejada según los términos establecidos por la plataforma, mismos términos que la mayoría de las personas no leen y aun así los aceptan. Sin embargo, no se establece una restricción precisa que protege

completamente al usuario, lo que genera incertidumbre sobre hasta qué punto se puede llegar a compartir esta información.

Asimismo, existe un capítulo dedicado a la seguridad de los datos personales en el cual se abordan temas cruciales para generar confianza y brindar mayor tranquilidad al dejar nuestros datos personales en manos de una tercera persona o en este caso una máquina. Se estipulan diversas normas que impone una responsabilidad sobre las personas encargadas de almacenar dicha información, lo que implica que las entidades que gestionan estos datos deben actuar con diligencia para protegerlos. Sin embargo, hay un punto especial que aún queda pendiente el cual es las nuevas innovaciones tecnológicas. Estas innovaciones, como la inteligencia artificial o los sistemas automatizados de procesamiento de datos carecen de un marco claro en cuanto a la firma de un contrato que especifique la responsabilidad de las partes involucradas. Es decir, no existe una base normativa estricta que regule que debe suceder si se produce un robo de información o si los datos son divulgados de manera no autorizada. Dado que estas innovaciones tecnológicas no cuentan con un acuerdo explícito de privacidad, no se puede precisar quien debe asumir la responsabilidad en caso de vulneraciones, lo que deja a los usuarios sin un mecanismo claro de protección o una acción que va a proteger sus datos cuando exista algún tipo de robo o usurpación de su información. De este modo, la falta de normativa rigurosa y un contrato que defina las responsabilidades en estos casos, pone en evidencia una de las lagunas más grandes en la regulación que debe ser abordada para garantizar una protección efectiva de los datos personales frente a las nuevas tecnologías.

1.2.2. Consecuencias de la ausencia de normativas en la gestión de datos.

La ausencia de normativas claras y robustas en la gestión de datos personales acarrea una serie de consecuencias que pueden afectar tanto a los usuarios como a las organizaciones encargadas de procesar dicha información. En primer lugar, se crea un vacío legal que permite que las entidades encargadas del tratamiento de datos puedan operar sin una supervisión estricta, lo que genera incertidumbre sobre la forma en que se manejan, protegen y comparten los datos personales. Este vacío provoca una falta de transparencia en los procesos, ya que los usuarios no tienen un conocimiento claro de cómo se utilizarán sus datos, ni las garantías de que estos serán manejados de manera responsable y segura.

También abre la puerta a posibles abusos o negligencias por parte de las entidades que procesan los datos. Si no existen reglas claras que definan las responsabilidades de quienes gestionan la información, es más probable que se produzcan incidentes de seguridad, como el robo de datos o la divulgación no autorizada de información sensible. Los usuarios, al no contar con un marco legal que proteja sus derechos, quedan expuestos a una vulnerabilidad constante, ya que no tienen la certeza de que se tomarán las medidas adecuadas para salvaguardar su privacidad.

Además, la falta de regulación genera un desajuste en la forma en que se implementan las tecnologías emergentes, como la inteligencia artificial, que procesan grandes volúmenes de datos personales. Estas tecnologías, al no estar sometidas a una normativa estricta, pueden operar sin el debido control, lo que puede llevar a decisiones automatizadas que afecten negativamente a los usuarios, sin que ellos puedan entender o cuestionar los procesos subyacentes. La falta de responsabilidad en estos casos también dificulta la identificación de culpables en caso de que se produzcan daños, como el robo de datos o la discriminación algorítmica.

Otra consecuencia importante es la pérdida de confianza en las plataformas y servicios que manejan datos personales. Si los usuarios perciben que sus datos no están siendo gestionados adecuadamente, es probable que se sientan miedo al compartir información, lo que podría obstaculizar el desarrollo de tecnologías basadas en datos y el progreso de muchos sectores. Esta desconfianza puede resultar en una resistencia al uso de servicios digitales, afectando el crecimiento y la innovación en diversas industrias.

También, la falta de normativas puede generar consecuencias económicas, ya que las empresas que no cumplen con estándares de protección de datos podrían enfrentar sanciones, pérdidas de reputación y demandas legales. Estas repercusiones no solo afectan la imagen de las organizaciones, sino que también generan costos adicionales que podrían haberse evitado con una correcta implementación de políticas de protección de datos.

1.3. Desafíos en su aplicación

1.3.1. Problemas en la supervisión y cumplimiento de la ley.

La supervisión y el cumplimiento de la ley en la gestión de datos personales presentan un desafío significativo, especialmente cuando el tratamiento de la información se realiza a través de medios tecnológicos, como aplicaciones y plataformas digitales. La naturaleza dinámica y compleja de la tecnología hace que sea extremadamente difícil implementar una supervisión eficaz sobre el uso y la protección de los datos, ya que los sistemas informáticos están en constante evolución y pueden operar de manera descentralizada, lo que complica la identificación y el control de los actores involucrados.

Uno de los principales problemas es que el entorno digital permite que los datos personales sean procesados de manera automática y en tiempo real por algoritmos y sistemas de inteligencia artificial, sin que los usuarios sean plenamente conscientes de cómo se utiliza su información. Esto, combinado con la escala masiva en la que se procesan los datos a través de las plataformas tecnológicas, dificulta la tarea de monitorear y verificar si las empresas están cumpliendo con las normativas de protección de datos.

Una posible solución para mejorar la supervisión en este contexto es la creación de aplicaciones especializadas que ayuden a las autoridades competentes a llevar un registro en tiempo real de las actividades de procesamiento de datos. Estas aplicaciones podrían permitir a las empresas y plataformas digitales reportar y documentar sus procesos de tratamiento de datos, generando un registro transparente que facilite la verificación de cumplimiento. Al integrar tecnologías como blockchain, se podría garantizar la inmutabilidad y la transparencia de la información proporcionada, haciendo que cualquier alteración o intento de ocultar el uso indebido de los datos sea fácilmente detectable.

Además, estas aplicaciones podrían ser utilizadas para realizar auditorías automáticas sobre el cumplimiento de las normas de seguridad y protección de datos personales, analizando los sistemas informáticos en busca de vulnerabilidades y riesgos. También podrían incluir alertas

automáticas en caso de que se detecten violaciones a la privacidad o incidentes de seguridad, lo que permitiría una respuesta rápida y eficiente ante cualquier problema.

Otra forma de regular la supervisión de los datos personales en un entorno tecnológico sería mediante la creación de marcos regulatorios específicos para el uso de tecnologías emergentes como la inteligencia artificial, la automatización y el análisis de grandes volúmenes de datos. Estas regulaciones podrían requerir que las empresas implementen sistemas de cumplimiento automático en sus plataformas, que permitan a las autoridades de protección de datos acceder de manera sencilla a la información relacionada con el tratamiento de los datos y verificar que se cumplen las normativas.

El desarrollo de tecnologías de monitoreo en tiempo real también podría contribuir a una mayor supervisión. Las herramientas de inteligencia artificial podrían ser utilizadas por las autoridades para analizar patrones de comportamiento en las plataformas digitales y detectar actividades sospechosas o el uso indebido de datos personales, sin necesidad de intervención humana constante.

El establecimiento de una plataforma centralizada o una red de aplicaciones interconectadas, en la que las empresas estén obligadas a registrar y actualizar regularmente el estado de sus actividades de tratamiento de datos, sería una medida efectiva para mejorar el cumplimiento de la ley. Esto permitiría a las autoridades de protección de datos tener una visión más clara y completa de las prácticas de las organizaciones y asegurarse de que se están tomando las medidas adecuadas para proteger la información personal de los usuarios.

1.3.2. Casos en los que la falta de regulación ha generado conflictos legales.

Debido a que existen muchísimas nuevas aplicaciones que usan la IA como modus operandi o modo de operación, se han generado muchas dudas sobre personas que pueden llegar a perder el empleo ya que sus funciones las puede realizar una aplicación o una plataforma de una forma más rápida y con menos gastos, es por ello que han existido casos donde se han generado disputas por falta de regulación de la IA es este el caso:

La IA generativa trabaja con estadística, no puede hacer arte": dibujantes, guionistas y actores de doblaje exigen más control en su uso y que no los sustituya Estos colectivos piden más seguridad y garantías para que se respeten sus derechos de autor ante la apropiación de la voz, de ilustraciones y de obras literarias para entrenar a esta tecnología Un estudio de Madrid convocó a varios actores y actrices de doblaje para que grabasen emociones", cuenta Raúl Lara, "yo fui uno de los que avisaron, leí las condiciones y pintaba a IA". El objetivo de aquel proyecto, argumenta, era captar voces para entrenar a la IA generativa. Finalmente, declinó la convocatoria. Esto ocurrió a comienzos de 2023 y fue el detonante para la creación de la Plataforma de Asociaciones y Sindicatos de Artistas de Voz en España (PASAVE) de la que es portavoz Raúl Lara. Ante la apropiación de la voz para vídeos hechos con IA o para entrenar a esta última, que han sufrido los profesionales del doblaje y de la locución, el colectivo consiguió incluir en la cesión de derechos la cláusula PASAVE: "Garantiza que no se utilice nuestra voz para educar IA ni para hacer clonaciones". Raúl Lara cuenta que ya la han incluido las principales distribuidoras como gigantes del streaming y canales de televisión. Pese a ello, Lara reconoce que el sector de los videojuegos se resiste: "Hay proyectos que no se están grabando a día de hoy porque los trabajadores se niegan a firmar una cesión de derechos que no les protejan". Sobre la locución publicitaria, Lara indica que "ha sido brutal" la merma de trabajo para los profesionales del sector: "Es un error usar voces sintéticas en un anuncio que busca conectar con el público al que se le pretende vender el producto o el servicio". La multinacional juguetera Toys R Us ha sido una de las primeras en lanzar spots publicitarios hechos con IA. También Coca Cola lanzó un anuncio la pasada Navidad desarrollados por esta tecnología. Imágenes sintéticas que también llegan a carteles de fiestas populares,

> portadas de libros e, incluso, utilizan las administraciones. El Ministerio de Juventud e Infancia retiró el año pasado la campaña del Día de la Niña en la Ciencia por usar imágenes artificiales que desataron las críticas de los ilustradores. "Somos conscientes del peligro que supone y de lo rápido que empresas y administraciones públicas han abrazado a la IA a costa de rebajar la calidad para ahorrar", cuenta David López, reconocido dibujante de cómics. Afea que dicha calidad de las obras las determine una tecnología que trabaja por estadística al no "entender los contextos": "Una viñeta no tiene sentido por sí misma, lo tiene con la anterior y la posterior". Además, el dibujante apunta al daño para el futuro de la profesión ya que la formación artística, en cualquiera de sus disciplinas, "es muy complicada y supone un largo camino hasta que encuentras la identidad como artista". Considera que se traduciría en una desmotivación para las nuevas generaciones si la IA arrebata el trabajo. (Ibañez, 2024)

Este debate sobre la IA generativa y su impacto en los sectores creativos, como el doblaje, la ilustración y la escritura, es uno de los más relevantes en la actualidad, y plantea varios problemas éticos, legales y profesionales. En mi opinión, el temor de los trabajadores de estos sectores es completamente válido. La IA generativa, al ser entrenada con datos que incluyen voces, imágenes y obras literarias, puede llegar a utilizar estos recursos sin el consentimiento adecuado de los creadores, lo que lleva a una especie de apropiación sin recompensar a quienes realmente producen el contenido original.

Uno de los puntos clave aquí es el hecho de que la IA no entiende ni valora el contexto, la emoción o el proceso artístico detrás de la creación. La IA trabaja por estadística, lo que significa que no tiene la capacidad de generar arte genuino, sino que reproduce patrones y combina datos existentes. Esto plantea la pregunta de si estamos dispuestos a permitir que una máquina sustituya la creatividad humana, que es un proceso complejo y lleno de matices, por una mera reproducción automatizada.

La creación de la Plataforma de Asociaciones y Sindicatos de Artistas de Voz en España (PASAVE*)*, muestra la necesidad urgente de regular el uso de la IA en el sector creativo. Es fundamental que se protejan los derechos de autor y se imponga un control en cuanto a la utilización de las voces, las ilustraciones y otros contenidos protegidos. Las cláusulas que prohíben el uso de estas voces para entrenar a la IA o crear "clonaciones" son un paso importante, pero como bien se menciona, aún queda mucho trabajo por hacer, especialmente con la resistencia de ciertos sectores, como los videojuegos.

Es alarmante ver cómo algunas empresas y gobiernos están utilizando IA para crear contenido, a menudo sin tener en cuenta la calidad artística o la implicación que esto tiene para los profesionales del sector. En lugar de avanzar hacia una integración respetuosa de la IA, estamos viendo una tendencia a usarla simplemente como una herramienta para reducir costos, sin valorar la repercusión que esto tendrá en el futuro de las profesiones creativas.

Además, el uso de voces sintéticas o imágenes generadas por IA en anuncios publicitarios, como en el caso de “Toys R Us” y “Coca-Cola”, demuestra cómo la IA está invadiendo incluso el ámbito comercial, con efectos dañinos para la conexión emocional entre la marca y el público. Las voces y las ilustraciones creadas por IA carecen de la calidez y autenticidad que los seres humanos pueden transmitir, lo que puede resultar contraproducente en el contexto de la publicidad, que depende en gran medida de la empatía y la relación con el consumidor.

Capítulo 2: Normativas internacionales y su aplicación a Ecuador.

2.1. GDPR y su enfoque en IA

2.1.1. Principios de la GDPR aplicables a la IA.

Dentro de la normativa que establece el GDPR no se encuentra por el momento completamente identificada a la IA, sin embargo es la única que ha tomado medidas o a tomado ímpetu en las decisiones que se dan de forma automatizada haciendo esto que exista una limitante para una plataforma o aplicación que use la IA dentro del articulo:

> Art. 22: Toma de decisiones individuales automatizadas, incluida la elaboración de perfiles. El interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de forma similar. El apartado 1 no se aplicará si la decisión: es necesaria para la celebración o ejecución de un contrato entre el interesado y un responsable del tratamiento; está autorizada por el Derecho de la Unión o de los Estados miembros al que esté sujeto el responsable y que también establezca medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos del interesado; o se basa en el consentimiento explícito del interesado. En los casos a que se refieren las letras a) y c) del apartado 2, el responsable del tratamiento aplicará las medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. Las decisiones a que se refiere el apartado 2 no se basarán en categorías especiales de datos personales a que se refiere el artículo 9, apartado 1, a menos que se aplique el artículo 9, apartado 2, letras a) o g), y existan medidas adecuadas para salvaguardar los derechos y libertades del interesado y sus intereses legítimos. (GDPR, 2018, pág. ART 22)

El Art. 22 del GDPR establece que las personas tienen el derecho a no ser sometidas a decisiones basadas exclusivamente en el procesamiento automatizado de sus datos, como el perfilado, que tenga efectos legales sobre ellas o las afecte significativamente. Sin embargo, hay excepciones, como cuando la decisión es necesaria para la ejecución de un contrato, está autorizada por la legislación de la Unión Europea, o se basa en el consentimiento explícito del individuo. En estos casos, el responsable del tratamiento debe implementar medidas para proteger los derechos de la persona, como ofrecer la posibilidad de intervención humana, permitir que se exponga su

punto de vista e impugnar la decisión. Además, las decisiones automatizadas no pueden basarse en categorías especiales de datos personales.

La relación de este artículo con la IA es crucial, ya que muchas aplicaciones de IA, como los algoritmos de perfilado y toma de decisiones automatizadas, pueden afectar directamente a las personas, por ejemplo, en ámbitos de crédito, seguros o empleo. En este sentido, el GDPR busca proteger a los individuos de posibles abusos o decisiones injustas tomadas por máquinas sin intervención humana.

En Ecuador, la legislación en protección de datos personales, como la Ley Orgánica de Protección de Datos Personales, aún no aborda de manera clara y detallada la regulación de decisiones automatizadas basadas en IA. Aunque se reconocen los derechos de los ciudadanos sobre sus datos, la legislación ecuatoriana carece de un marco robusto que regule específicamente el perfilado y las decisiones automatizadas, así como la intervención humana en dichos procesos. La falta de infraestructura adecuada para garantizar la transparencia, justicia y no discriminación en el uso de IA refleja una necesidad de fortalecer la legislación para proteger mejor a los ciudadanos en el contexto actual de avances tecnológicos.

Así mismo existe este otro artículo el cual menciona:

> "Art. 5: Principios relativos al tratamiento de datos personales Los datos personales serán: tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia"); recopilados con fines específicos, explícitos y legítimos, y no tratados ulteriormente de manera incompatible con dichos fines; el tratamiento ulterior con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos no se considerará, de conformidad con el Artículo 89(1), incompatible con los fines iniciales ("limitación de la finalidad"); adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan ("minimización de datos"); exactos y, cuando sea necesario, actualizados; se deben tomar todas las medidas razonables para

> garantizar que los datos personales que sean inexactos, teniendo en cuenta los fines para los que se tratan, se supriman o rectifiquen sin dilación ("exactitud"); conservados de una forma que permita la identificación de los interesados durante no más tiempo del necesario para los fines para los que se tratan los datos personales; Los datos personales podrán conservarse durante periodos más largos siempre que se traten únicamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sujeto a la aplicación de las medidas técnicas y organizativas apropiadas exigidas por el presente Reglamento para salvaguardar los derechos y libertades del interesado («limitación del plazo de conservación»); se tratarán de forma que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daños accidentales, mediante medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). El responsable del tratamiento será responsable del cumplimiento del apartado 1 («rendición de cuentas») y podrá demostrarlo. (GDPR, 2018, pág. ART 5)

El Art. 5 del GDPR establece principios clave para el procesamiento de datos personales: Deben ser tratados de manera legal, justa y transparente, recolectados para fines específicos y legítimos, y no procesados de manera incompatible con esos fines. Además, los datos deben ser adecuados, relevantes y limitados a lo necesario para los fines previstos, generando una referencia a la minimización de datos. También se garantiza que los datos sean exactos, actualizados y almacenados solo el tiempo necesario dando una limitación del almacenamiento, además de ser procesados de forma segura lo cual genera mayor integridad y confidencialidad. Finalmente, el responsable del tratamiento debe demostrar que cumple con estos principios implicando una responsabilidad.

Estos principios son fundamentales en el contexto de la IA, ya que el uso de algoritmos para tomar decisiones automatizadas o procesar grandes volúmenes de datos personales debe

alinearse con ellos. Por ejemplo, la transparencia en el uso de IA es crucial, ya que los usuarios deben ser informados sobre cómo se procesan sus datos. Además, la minimización de datos asegura que solo se procesen los datos necesarios para el funcionamiento de los algoritmos, evitando el procesamiento excesivo de información personal.

En Ecuador, aunque la Ley Orgánica de Protección de Datos Personales, busca regular la protección de datos, aún existen vacíos en la regulación sobre el uso de IA y el procesamiento automatizado de datos. La falta de un marco específico para el uso de IA en la toma de decisiones y el procesamiento de datos personales limita la implementación de principios como la transparencia y la limitación del almacenamiento. Además, no se han establecido mecanismos claros para garantizar la seguridad de los datos procesados por IA ni para auditar el cumplimiento de estos principios en el ámbito de la inteligencia artificial. Esto muestra la necesidad de fortalecer la legislación ecuatoriana para garantizar una protección más robusta frente al uso de tecnologías emergentes como la IA.

> Art. 6: Licitud del tratamiento El tratamiento solo será lícito si y en la medida en que se cumpla al menos una de las siguientes condiciones: el interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o más fines específicos; el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; el tratamiento es necesario para el cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento; el tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física; el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, salvo que prevalezcan sobre dichos intereses los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el

interesado sea un niño. La letra f) del párrafo primero no se aplicará al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. Los Estados miembros podrán mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento en lo que respecta al tratamiento, a efectos del cumplimiento de las letras c) y e) del apartado 1, determinando con mayor precisión los requisitos específicos para el tratamiento y otras medidas destinadas a garantizar un tratamiento lícito y leal, incluso para otras situaciones específicas de tratamiento, tal como se establece en el capítulo IX. 1. La base jurídica para el tratamiento a que se refieren las letras c) y e) del apartado 1 se establecerá mediante: el Derecho de la Unión; o el Derecho de los Estados miembros al que esté sujeto el responsable del tratamiento. 2. La finalidad del tratamiento se determinará en dicha base jurídica o, en lo que respecta al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de la autoridad pública conferida al responsable del tratamiento. 3. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de las normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto del tratamiento; los interesados afectados; las entidades a las que se pueden comunicar los datos personales y los fines para los que se pueden comunicar; la limitación de la finalidad; los periodos de conservación; y las operaciones y procedimientos de tratamiento, incluidas las medidas para garantizar un tratamiento lícito y leal, como las aplicables a otras situaciones específicas de tratamiento previstas en el capítulo IX. 4El Derecho de la Unión o de los Estados miembros deberá perseguir un objetivo de interés público y ser proporcionado al fin legítimo perseguido. Cuando el tratamiento para un fin

> distinto de aquel para el que se han recogido los datos personales no se base en el consentimiento del interesado ni en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcionada en una sociedad democrática para salvaguardar los objetivos a que se refiere el artículo 23, apartado 1, el responsable del tratamiento, a fin de determinar si el tratamiento para otro fin es compatible con el fin para el que se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas: cualquier vínculo entre los fines para los que se han recogido los datos personales y los fines del tratamiento posterior previsto; el contexto en el que se han recogido los datos personales, en particular en lo que respecta a la relación entre los interesados y el responsable del tratamiento; la naturaleza de los datos personales, en particular si se tratan categorías especiales de datos personales, de conformidad con el artículo 9, o si se tratan datos personales relacionados con condenas e infracciones penales, de conformidad con el artículo 10; las posibles consecuencias del tratamiento posterior previsto para los interesados; la existencia de garantías adecuadas, que pueden incluir el cifrado o la seudonimización. (GDPR, 2018, pág. ART 6)

El principio de licitud del procesamiento en el GDPR establece que el tratamiento de datos personales solo es legal si se cumple al menos una de las siguientes condiciones: el consentimiento del titular, la necesidad contractual, el cumplimiento de obligaciones legales, la protección de intereses vitales, el interés público o el ejercicio de autoridad oficial, o un interés legítimo del responsable del tratamiento que no vulnere los derechos del titular. Además, la normativa permite que los Estados miembros adapten la regulación para garantizar un tratamiento justo y lícito, estableciendo condiciones específicas como los plazos de almacenamiento, los tipos de datos tratados y los procedimientos de procesamiento. Este principio es esencial en el uso de la IA, ya que muchas aplicaciones dependen del procesamiento masivo de datos para entrenar algoritmos, tomar decisiones automatizadas y hacer perfilado.

La IA plantea desafíos sobre el consentimiento, ya que en muchos casos los datos son utilizados para fines no previstos originalmente, lo que requiere evaluar la compatibilidad del nuevo procesamiento con el propósito inicial. Además, el uso de datos sensibles (como los de salud o biométricos) requiere garantías adicionales, como el uso de cifrado, para evitar riesgos de discriminación o uso indebido de la información.

En Ecuador, la Ley Orgánica de Protección de Datos Personales, también establece que el procesamiento de datos debe ser lícito, pero no desarrolla de manera específica cómo se aplica este principio en el contexto de la IA. Hay varias brechas en la regulación ecuatoriana: Falta de regulación específica sobre IA ya que no se detallan reglas claras sobre el uso de IA para el tratamiento automatizado de datos ni cómo garantizar la transparencia y equidad en las decisiones algorítmicas, debilidad en la exigencia de consentimiento informado, puesto que la LOPDP reconoce la importancia del consentimiento, pero no establece mecanismos exhaustivos para garantizar que las personas comprendan cómo sus datos pueden ser utilizados por sistemas de IA, la protección insuficiente frente a decisiones automatizadas, debido que no hay normativas claras que establezcan el derecho de los ciudadanos a impugnar decisiones tomadas por IA ni a exigir intervención humana en procesos que puedan afectar sus derechos, falta de medidas de seguridad específicas para IA ya que no se detallan protocolos obligatorios para el uso de cifrado, anonimizarían en el procesamiento automatizado de datos, lo que podría exponer a los ciudadanos a mayores riesgos. Es por ello que el GDPR establece criterios claros para la licitud del procesamiento y la regulación de tecnologías como la IA, esto debería tomar como base el Ecuador debido a que aún falta una regulación específica que contemple los desafíos de la inteligencia artificial en el tratamiento de datos personales.

> Art. 35: Evaluación de impacto de la protección de datos 1. Cuando sea probable que un tipo de tratamiento, en particular el que utiliza nuevas tecnologías, y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, entrañe un alto riesgo para los derechos y las libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales. 2. Una única evaluación

podrá abordar un conjunto de operaciones de tratamiento similares que presenten altos riesgos similares. El responsable del tratamiento solicitará el asesoramiento del delegado de protección de datos, cuando este haya sido designado, al realizar una evaluación de impacto de la protección de datos. La evaluación de impacto de la protección de datos a que se refiere el apartado 1 se requerirá, en particular, en caso de: una evaluación sistemática y exhaustiva de aspectos personales relativos a las personas físicas que se base en el tratamiento automatizado, incluida la elaboración de perfiles, y en la que se basen decisiones que produzcan efectos jurídicos sobre la persona física o que la afecten significativamente de forma similar; el tratamiento a gran escala de categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10; o una monitorización sistemática a gran escala de un área de acceso público. 1. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento sujetas al requisito de una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. 2. La autoridad de control comunicará dichas listas al Comité a que se refiere el artículo 68. 1. La autoridad de control también podrá establecer y publicar una lista de los tipos de operaciones de tratamiento para las que no se requiere una evaluación de impacto relativa a la protección de datos. 2. La autoridad de control comunicará dichas listas al Comité. Antes de la adopción de las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia a que se refiere el artículo 63 cuando dichas listas impliquen actividades de tratamiento relacionadas con la oferta de bienes o servicios a los interesados o con la monitorización de su comportamiento en varios Estados miembros, o puedan afectar sustancialmente a la libre circulación de datos

personales dentro de la Unión. La evaluación contendrá, como mínimo: una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, incluido, en su caso, el interés legítimo perseguido por el responsable; una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento en relación con los fines; una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1; y las medidas previstas para abordar los riesgos, incluidas las salvaguardias, medidas de seguridad y mecanismos para garantizar la protección de los datos personales y demostrar el cumplimiento del presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y otras personas afectadas. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por parte de los responsables o encargados pertinentes se tendrá debidamente en cuenta al evaluar el impacto de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de una evaluación de impacto sobre la protección de datos. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes sobre el tratamiento previsto, sin perjuicio de la protección de los intereses comerciales o públicos ni de la seguridad de las operaciones de tratamiento. Cuando el tratamiento con arreglo al artículo 6, apartado 1, letras c) o e), tenga base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro al que esté sujeto el responsable, dicho Derecho regule la operación de tratamiento específica o el conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto sobre la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no se aplicarán, a menos que los Estados miembros consideren necesario realizar dicha evaluación antes de las actividades de tratamiento. Cuando sea necesario, el

> responsable realizará una revisión para evaluar si el tratamiento se realiza de conformidad con la evaluación de impacto sobre la protección de datos, al menos cuando se produzca un cambio en el riesgo que representan las operaciones de tratamiento. (GDPR, 2018, pág. ART 35)

El Análisis de Impacto en la Protección de Datos (DPIA), establecido en el GDPR, es un procedimiento obligatorio cuando el procesamiento de datos, especialmente con nuevas tecnologías como la IA, representa un alto riesgo para los derechos y libertades de las personas. Se debe realizar antes del tratamiento de datos y evaluar el impacto en la privacidad. Es especialmente necesario en casos de decisiones automatizadas con efectos legales o significativos, procesamiento masivo de datos sensibles y monitoreo sistemático de espacios públicos. Además, las autoridades de protección de datos deben establecer listas de tratamientos que requieren o no un DPIA.

El uso de IA en el procesamiento de datos personales plantea grandes retos en este ámbito. Los algoritmos pueden tomar decisiones basadas en perfiles automatizados, lo que podría afectar derechos fundamentales sin intervención humana clara. El DPIA es clave para garantizar que estos sistemas respeten principios de transparencia, minimización de datos y seguridad. Además, permite evaluar riesgos de sesgos algorítmicos, discriminación o uso indebido de datos personales.

En Ecuador, la Ley Orgánica de Protección de Datos Personales reconoce la necesidad de evaluar riesgos en el tratamiento de datos, pero no desarrolla de manera específica la obligación de realizar un DPIA antes de implementar tecnologías como la IA. Existen varios vacíos en la legislación ecuatoriana como la falta de obligatoriedad clara del DPIA puesto que no se establece que los proyectos de IA deban realizar un análisis de impacto en la protección de datos antes de su implementación, la ausencia de regulaciones específicas para IA y perfilamiento automatizado ya que no hay normas que exijan una evaluación de riesgos de sesgos y transparencia en los modelos de IA, la supervisión limitada debido a que no se han definido listas de tratamientos de alto riesgo que requieran obligatoriamente un DPIA, como sí ocurre en el GDPR, la falta de mecanismos de consulta pública ya que en el GDPR se recomienda que los responsables del tratamiento consulten con los titulares de datos, algo que la LOPDP no exige de manera específica para IA y la Carencia

de auditorías y revisiones periódicas esto porque no se exige revisar regularmente los sistemas automatizados para garantizar su conformidad con la normativa de protección de datos.

Es por ello que debemos tomar como base al GDPR, debido a que tienen a enfocar de forma más específica su normativa llegando a generar un convenio con la IA, así mismo dándole una limitante y un control, mismo control que dentro de nuestro Estado no se tiene.

> Art. 32: Seguridad del tratamiento Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y las libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras, según corresponda: la seudonimización y el cifrado de los datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; la capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico; un proceso para probar, evaluar y valorar periódicamente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. Al evaluar el nivel adecuado de seguridad, se tendrán en cuenta en particular los riesgos que presenta el tratamiento, en particular la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilícito a datos personales transmitidos, almacenados o tratados de otro modo. La adhesión a un código de conducta aprobado, como se menciona en el artículo 40, o a un mecanismo de certificación aprobado, como se menciona en el artículo 42, podrá utilizarse como elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo. El responsable y el encargado del tratamiento adoptarán medidas para garantizar que cualquier persona física

> que actúe bajo la autoridad del responsable o del encargado y que tenga acceso a datos personales no los trate salvo siguiendo instrucciones del responsable, salvo que esté obligada a hacerlo por el Derecho de la Unión o de los Estados miembros. (GDPR, 2018, pág. ART 32)

La seguridad en el procesamiento de datos dentro del marco del GDPR exige que los responsables y encargados de los datos implementen medidas adecuadas para garantizar la protección de la información personal considerando los riesgos existentes y los avances tecnológicos. Estas medidas incluyen el cifrado de datos la garantía de confidencialidad e integridad de los sistemas el establecimiento de mecanismos de recuperación en caso de incidentes y la realización de pruebas periódicas para evaluar la efectividad de las estrategias de seguridad.

La inteligencia artificial introduce desafíos adicionales en la seguridad del procesamiento de datos ya que maneja grandes volúmenes de información y utiliza algoritmos de aprendizaje automático que pueden ser vulnerables a ataques, filtraciones o sesgos. La falta de transparencia en algunos modelos de IA dificulta el control sobre la seguridad y el cumplimiento normativo además de que el uso de IA puede aumentar los riesgos de identificación de datos anonimizados lo que hace indispensable la implementación de medidas avanzadas de protección.

En Ecuador la normativa de protección de datos aún no cuenta con regulaciones específicas para la inteligencia artificial ni con estándares claros sobre medidas de seguridad avanzadas. No existe una exigencia clara de cifrado en todos los casos ni un marco de auditoría periódica que permita evaluar la seguridad del tratamiento automatizado de datos. Tampoco se han desarrollado certificaciones o códigos de conducta aprobados como en la Unión Europea lo que dificulta la supervisión efectiva de los sistemas de IA y el cumplimiento de estándares internacionales de protección de datos.

Para fortalecer la seguridad del procesamiento de datos en el país es fundamental establecer regulaciones que aborden los riesgos específicos de la inteligencia artificial incluyendo la obligatoriedad de pruebas de seguridad, el uso de medidas avanzadas de protección de datos y la

implementación de mecanismos de supervisión y auditoría que permitan garantizar la protección de los derechos de los ciudadanos en un entorno digital en constante evolución.

2.1.2. ¿Cómo regula la GDPR la toma de decisiones automatizadas?

Dentro del Reglamento General de Protección de Datos, este regula la toma de decisiones automatizadas, incluyendo el perfilado, en su artículo 22, del cual hablamos anteriormente y lo citamos para que exista una mayor entendimiento, se puede entender que este artículo es muy importante para la investigación de nuestra tesis, debido a que dentro de este punto se toma un conflicto, que es la toma de decisiones automatizadas, y cómo prevenir el mismo, ya que no se puede llegar a tener un conocimiento básico de sobre quien recae las preguntas o la información que se guarda y almacena dentro de su base de datos. Este artículo establece que los individuos tienen el derecho a no ser objeto de una decisión basada únicamente en el procesamiento automatizado de datos, sino que dicha decisión debe tener efectos legales o un impacto significativo en ello, puesto que la misma al ser de carácter automatizado no se puede sobre entender si existe, o no una vulneración de los derechos de la persona.

Las regulaciones del Reglamento General de Protección de Datos permiten excepciones a la prohibición de decisiones automatizadas en tres casos específicos. Primero cuando la automatización es esencial para la ejecución de un contrato entre la persona y una empresa u organización. Segundo si una ley de la Unión Europea o de un Estado miembro, autoriza este tipo de procesamiento y establece medidas de protección para los afectados. Tercero cuando la persona ha dado su consentimiento explícito para que sus datos sean tratados de esta manera. En cualquiera de estos escenarios, es obligatorio aplicar salvaguardas para que se pueda llegar a solventar los derechos de las personas frente a los de la empresa o de las bases de datos las cuales almacenan la información personal de la persona que está siendo intervenido.

Además, el Reglamento General de Protección de Datos establece restricciones adicionales cuando se trata de datos que son de carácter sensible, como información sobre salud, raza, religión u opiniones políticas. Sólo en estas circunstancias las cuales son la excepción a regla general y con medidas de seguridad reforzadas se permite el uso de estos datos en decisiones las cuales son automatizadas. Esta regulación es clave en el contexto de la inteligencia artificial ya que muchos aplican de forma automatizada las decisiones que toma la IA y está en varias ocasiones puede

afectar a lo que son las personas, como la concesión de créditos, procesos de contratación laboral o la determinación de tarifas de seguros. La normativa busca garantizar transparencia en estos sistemas, asegurando que los ciudadanos sepan ¿Cuándo? y ¿Cómo? la inteligencia artificial está procesando sus datos y de qué criterios se utilizan en la toma de dicha decisión, especificando así de una forma clara para que no exista una vulneración de derechos sobre las personas es por ello que la transparencia en estos sistemas es un eje fundamental para el manejo de la misma.

Como ya tenemos un conocimiento previo de que dentro de nuestra nación es decir en Ecuador aún no existe una legislación específica que regula algún tipo de toma de decisión automática ni disponemos que otorguen a los ciudadanos derechos similares a los que son establecidos en el artículo 22 del Reglamento General de Protección de Datos, no hay entonces mecanismos que obliguen a la intervención humana en estos procesos, ni, ningún tipo de regulación clara sobre el uso de la inteligencia artificial en el manejo y la gestión de los datos que son personales, es decir de carácter privado. Esta falta de normativa deja a los ciudadanos expuestos a posibles decisiones injustas o discriminatorias sin una posibilidad de apelar por la misma. Para garantizar una adecuada protección de los derechos en esta era que es sumamente de carácter digital, es fundamental desarrollar un marco legal que ponga una limitante y controle el uso de la inteligencia artificial en la toma de decisiones automatizadas, estableciendo controles, transparencia y mecanismos de supervisión que prevengan abusos y aseguren la equidad en el tratamiento de los datos personales, o se puede optar por algún tipo de ente regulador el cual maneje y controle estos sistemas.

2.2. Ejemplos de otros países

2.2.1. Regulación de IA en el régimen europeo.

España es uno de los países más grandes en el mundo, y también es un país muy desarrollado, es por eso que da pasos gigantes en el nuevo mundo digital, es por ello que ya proponen nuevos, ordenamientos y entes reguladores como:

El Gobierno ha aprobado este martes en el Consejo de ministros el estatuto de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA). Este nuevo

> organismo se adscribe al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, como indica Moncloa en un comunicado de este martes. Con la creación de esta Agencia, España se convierte en el primer país europeo en tener un órgano de estas características y se anticipa a la entrada en vigor del Reglamento Europeo de Inteligencia Artificial. Este reglamento establecerá para los Estados miembros la obligación de seleccionar una 'autoridad nacional de supervisión' que se encargue de controlar la aplicación de la normativa en materia de Inteligencia Artificial. (RTVE, 2023)

La aprobación del estatuto de la agencia española de supervisión de la inteligencia artificial es uno de los más grandes pasos que se puede dar para un ordenamiento y un control de la inteligencia artificial, esto por parte del gobierno de España representa un hito en la regulación de la inteligencia artificial dentro de la Unión Europea. Con su creación, España se convierte en el primer país en establecer un organismo de supervisión específico para la inteligencia artificial, Adelantándose a la entrada en vigor del reglamento europeo de inteligencia artificial. Este marco normativo exigirá que el estado y cada uno de los estados miembros designe una autoridad nacional la cual sea responsable de supervisar el cumplimiento de la normativa que tienen como materia.

La creación de la Agencia Española de Supervisión de la Inteligencia Artificial supone un avance en términos de transparencia y a su vez de seguridad en la implementación y desarrollo y a su vez en la aplicación de la inteligencia artificial, esto debido a que su integración dentro del ministerio de asuntos económicos y transformación digital, que es conocido dentro del reglamento de España y a través de la secretaría de Estado de digitalización e inteligencia artificial, se busca garantizar una regulación alineada con todas las políticas de transformación digital del país. Esto responde a la necesidad de establecer ciertos tipos de controles sobre los sistemas informáticos especialmente los cuales brindan información y contenido digital automatizado, lo cual genera una inteligencia artificial, esto con el fin de mitigar ciertos riesgos como sesgos algorítmicos, falta de aplicabilidad de las decisiones automatizadas y potenciales vulneraciones de derechos que son fundamentales para los individuos.

Sin embargo, la efectividad de la Agencia Española de Supervisión de Inteligencia Artificial va a depender mucho de diversos factores, uno de ellos es su grado de independencia, este será clave dentro de este punto, puesto que para evitar interferencias políticas o económicas que puedan comprometer su imparcialidad en la supervisión, será uno de los puntos que tiene que entrar en debate, también es fundamental que cuente con recursos suficientes, tanto en términos de presupuesto como de personal especializado, ya que esta inteligencia no deja de avanzar y no deja de asumir riesgos y sesgos como vacíos legales que no se pueden llegar a dejar en la nada. También debe encontrar un equilibrio entre la regulación y fomento de la innovación ya que un marco excesivamente restrictivo podría desincentivar el desarrollo tecnológico y la inversión que genera la ahí adentro del país.

Al momento en el cual entra en vigor el reglamento de inteligencia artificial de la Unión Europea también marca uno de los avances más importantes dentro de la regulación tecnológica a nivel mundial. Esto debido a que se trata de la primera normativa integral diseñada para garantizar que la inteligencia artificial desarrollada y utilizada dentro del territorio europeo sea confiable y respetuosa con los derechos que son fundamentales y que tiene cada persona desde que nace. Este marco regula y busca armonizar un mercado interno de inteligencia artificial que sea comprensible y que sea de carácter sano para que pueda adoptar cualquier tipo de postura y no vulnere derechos importantes como lo que son la seguridad transparencia y supervisión.

Uno de los elementos claves dentro de esta regulación, es la clasificación de los sistemas de inteligencia artificial según el nivel de riesgo esto puesto que suponen que un riesgo inaceptable va a ser prohibido de forma inmediata como también podrá existir lo que son altos riesgos que estarán sujetos a requisitos de supervisión y control. Además, se han establecido mecanismos para regularizar los modelos de inteligencia artificial que son de forma general o de propósito general como aquellos son utilizados en aplicaciones de gran alcance cómo puede ser el ChatGPT que es uno de los más usados a nivel mundial.

En términos también de gobernanza y de la supervisión el reglamento establece una estructura de organismos que garantizarán una correcta implementación. Esto a nivel de que la Unión Europea y la oficina de inteligencia artificial de la Comisión Europea será el ente principal el cual va a ser encargado de hacer cumplir con toda la normativa que se encuentre dentro de la ley. Cada estado miembro tiene hasta el 2 de agosto de 2025 para designar sus propias autoridades

nacionales competentes los mismos que serán responsables de la supervisión y vigilancia del mercado en sus respectivos territorios. En España esta función recaerá en la Agencia Española de Supervisión de la Inteligencia Artificial, el cual es un organismo que ya se ha adelantado a la entrada de vigor de la normativa europea.

También se comprende que va a existir un régimen sancionador el cual van a tener e imponer multas severas para quienes incumplan las disposiciones que se encuentran establecidas dentro de la normativa y menciona que las sanciones pueden llegar hasta el 7% de la facturación anual global esto para las violaciones más graves.

Este reglamento me parece un avance muy grande significativo para todo el mundo no solo para lo que es su estado debido a que ya pone un iniciativa la cual cualquier país del mundo puede tomar para desarrollar un reglamento, que puede basarse en el mismo en el cual se va a interponer la Unión Europea o crear uno según su estado pero ya advierte de ciertas actividades ilícitas que puede llegar a generar la inteligencia artificial y así mismo impone que los estados también avancen con esta normativa y puedan llegar a generar un reglamento para poner una limitante a la inteligencia artificial.

2.2.2. Enfoque de Canadá y Brasil en la regulación de IA.

En el contexto de regulación sobre la inteligencia artificial en Canadá hasta la fecha no se ha contado con ningún tipo de legislación específica dedicada exclusivamente a la inteligencia artificial, sin embargo, el país ha implementado varias iniciativas y marcos regulatorios que abordan aspectos relacionados con el desarrollo del uso de la inteligencia artificial más específica en la tecnología. Por ejemplo, existen directrices y marcos éticos como, el cual, el gobierno canadiense ha publicado diversas directrices éticas para el uso de la inteligencia artificial en el sector público, enfatizando principios como la transparencia, la responsabilidad, la equidad, etc. Estas directrices buscan garantizar que los sistemas de diligencia artificial respeten los derechos fundamentales y promuevan el bienestar social.

A su vez algunas provincias han pedido o han propuesto una implementación de legislaciones que abordan aspectos relacionados con la IA sin embargo todavía no se ha determinado ningún cierto tipo de regularización estrictamente enfocado en la inteligencia artificial y los sistemas con respuestas automatizadas o funciones automatizadas.

> El 10 de diciembre de 2024, “Abramus” informaba de la aprobación del Proyecto de Ley 2338/2023, que propone la creación de un marco regulatorio para la inteligencia artificial en Brasil. El Proyecto de Ley ha sido iniciativa del presidente de la Cámara, Rodrigo Pacheco, y ha tenido como relator al senador Eduardo Gomes. Este proyecto legislativo busca establecer las reglas que han de regir el desarrollo de sistemas de inteligencia artificial que, además de asegurar una IA responsable, deben, necesariamente, garantizar el respeto de los derechos de quienes, con sus obras y prestaciones, hacen posible el desarrollo de modelos de IA. Ahora, el Proyecto de Ley ha de ser sometido a votación en la Cámara de Diputados. Abramus, Asociación Brasileña de Música y Artes, y Autvis, Asociación Brasileña de Derechos de Autor Visual, han defendido desde el principio la aprobación de este Proyecto, en el texto de su relator, por entender que los creadores necesitan y merecen que se protejan y respeten sus respectivos derechos de autor. En una nota conjunta con varias entidades de la industria creativa, Abramus y Autvis destacaron que la inteligencia artificial es un eje fundamental para el desarrollo social y económico del país. En la misma medida, es fundamental proteger los derechos de los creadores, garantizando un mayor control de sus obras. (Mendez, 2025)

La aprobación del proyecto de ley por parte del Senado de Brasil marca un paso muy relevante en la regulación de la inteligencia artificial especialmente en el país de Brasil, debido a que esta iniciativa impulsa cómo establecer un marco normativo para el desarrollo de los sistemas que utilizan la inteligencia artificial haciendo que este garantice tanto la responsabilidad en su implementación como el respeto a los derechos de los creadores de contenido y obras protegidas por derechos de autor, esta propuesta de ley se basa más en una protección para los artistas o personas que utilizan medios artísticos para ganarse un sustento diario debido a que con el uso de la inteligencia artificial muchos de estos artistas se han quedado sin trabajo debido a que les puede reemplazar una computadora, aplicación, tecnología, etc., la cual cuente con algún programa

automatizado para alguna función, por ejemplo muchos de los dibujantes se han quedado sin empleo debido a que una máquina puede producir cualquier tipo de dibujo que ellos le pidan.

Uno de los aspectos más destacados del proyecto en su énfasis en la protección de los derechos de autor en el contexto de la inteligencia artificial es la creciente capacidad de los sistemas de inteligencia artificial, para generar contenido basado en obras preexistentes, debido a esto se ha generado un gran debate sobre la necesidad de garantizar que los creadores reciban un reconocimiento y una compensación justa por el uso de sus trabajos. En este sentido la asociación brasileña de música y artes "Abramus" han defendido la iniciativa argumentando que la regulación debe equilibrar el desarrollo tecnológico con la protección de los derechos de los autores y artistas.

Este proyecto también subraya la importancia de la inteligencia artificial como motor de desarrollo social económico en Brasil, debido a que esta regulación no sólo busca mitigar riesgos asociados a un uso indebido, sino que también fomenta un entorno de innovación responsable que impulse la competitividad del país en el ámbito digital. Actualmente este proyecto debe ser sometido a votación de la Cámara de Diputados su aprobación y posterior aplicación serán claves para determinar si Brasil logra consolidar un modelo regulatorio equilibrado.

Capítulo 3: Riesgos éticos del uso de IA en datos personales

3.1. Sesgo algorítmico y discriminación

3.1.1. ¿Cómo surgen los sesgos en los algoritmos de IA?

Para entender un poco más este tema de los riesgos de la IA debemos saber que es un sesgo algorítmico, es por eso que tenemos el siguiente análisis:

> El sesgo algorítmico se produce cuando los errores sistemáticos de los algoritmos de machine learning producen resultados injustos o discriminatorios. A menudo, refleja o refuerza los prejuicios socioeconómicos, raciales y de género existentes. Los sistemas de inteligencia artificial (IA) emplean algoritmos para descubrir patrones en los datos, o para predecir valores de salida a partir de un conjunto determinado de variables de entrada. Los algoritmos sesgados pueden afectar estos patrones y resultados de maneras que conduzcan

> a decisiones o acciones perjudiciales, promuevan o perpetúen la discriminación y la desigualdad, y erosionen la confianza en la IA y en las instituciones que la utilizan. Estos impactos pueden crear riesgos legales y financieros para las empresas. Por ejemplo, según la Ley de IA de la UE, el incumplimiento de sus prácticas prohibidas de IA puede significar multas de hasta 35 000 000 EUR o el 7 % de la facturación anual mundial, lo que sea mayor. El sesgo algorítmico es especialmente preocupante cuando se encuentra dentro de los sistemas de IA que respaldan decisiones que alteran la vida en áreas, como la atención médica, la aplicación de la ley y los recursos humanos. El sesgo puede entrar en los algoritmos de muchas maneras, como datos de entrada de entrenamiento sesgados o limitados, decisiones de programación subjetivas o interpretación de resultados. La mitigación del sesgo algorítmico comienza con la aplicación de los principios de gobernanza de la IA, incluida la transparencia y la aplicabilidad, a lo largo de todo el ciclo de vida de la IA. (Jonker & Julie, 2024)

Teniendo un conocimiento más ampliado gracias a la definición que pudimos entender entonces conocemos que el sesgo algorítmico es un problema crítico, porque nos dice que puede afectar la equidad dentro de las decisiones tomadas por lo que son los sistemas de inteligencia artificial aquí nos menciona que los algoritmos de “Machine Learning” los cuales están diseñados para encontrar patrones en lo que son los datos en algunos momentos pueden terminar reforzando prejuicios existentes debido a datos sesgados o decisiones de diseño que son incorrectas y que no son las que estamos pidiendo es decir nos dan una información errónea sobre lo que queremos informarnos. Además, la presencia de estos sesgos nos puede llevar a tener consecuencias legales y financieras para las empresas que implementan algunas de las tecnologías que cuentan con inteligencia automatizada, es por eso que debe ser esencial que se incorpora en principios de gobernanza en la inteligencia artificial porque gracias a eso podemos mitigar estos sesgos y se puede garantizar la transparencia dentro de todo el proceso.

Es indudable que la inteligencia artificial tiene uno de los potenciales más grandes e increíbles que se ha logrado conocer dentro de nuestra era, pero también presenta uno de los desafíos éticos más significativos debido al gran compromiso y gran vacío que todavía se debe conocer. Si los sesgos no se abordan adecuadamente puede llegar a generar una desigualdad social es por eso que como mencionamos anteriormente la transparencia debe ser una de los métodos y de las bases que se tienen que centrar para regularizar la inteligencia artificial.

Sesgos en los datos

Los datos defectuosos se caracterizan por ser no representativos, carecer de información, estar históricamente con sesgo o ser "deficientes". Esto conduce a algoritmos que producen resultados parciales y amplifican cualquier sesgo en los datos. Los sistemas de IA que emplean resultados con sesgo como datos de entrada para la toma de decisiones crean un ciclo de retroalimentación que también puede reforzar el sesgo con el tiempo. Este ciclo, en el que el algoritmo aprende continuamente y perpetúa los mismos patrones con sesgo, conduce a resultados cada vez más sesgados. También pueden surgir sesgos durante la fase de entrenamiento si los datos se categorizan o evalúan incorrectamente. A veces, los algoritmos pueden "aprender" de la correlación de datos en lugar de la causalidad, ya que no poseen la capacidad de comprender la diferencia. Cuando esto sucede, el resultado del algoritmo puede estar sesgado en el sentido de que el modelo no consideró otros factores en los datos que pueden ser de mayor importancia. Un ejemplo comúnmente citado de sesgo de correlación es un modelo hipotético que determina una relación causal entre el aumento de los ataques de tiburones y el incremento de las ventas de helados. En realidad, ambas situaciones suelen darse durante el verano y sólo poseen una relación correlativa. (Jonker & Julie, 2024)

Este sesgo de los datos ocurre al momento en el cual los datos que mencionamos son utilizados para entrenar los algoritmos y estos algoritmos no son representativos lo que puede generar decisiones automatizadas que sean de carácter injusto para lo que se pidió, es por ello que estos algoritmos pueden aprender patrones incorrectos y los datos tienen correlaciones en algún tipo de causal lo que puede producir predicciones erróneas o sesgadas como estamos informándonos. El ciclo de retroalimentación que se describe es el que puede perpetuar estos sesgos a lo largo del tiempo es por eso que muchas de las decisiones que a veces son tomadas por estas inteligencias automatizadas pueden llegar a tener errores muy grandes los cuales nosotros no vamos a poder tener el conocimiento, debido a que nosotros buscamos una información acertada.

Es por ello que yo considero que debe ser fundamental que los datos sean representativos y reflejen la diversidad de la población, para evitar que estos sesgos ocurran debe ser necesario realizar una revisión constante de los datos y aplicar lo que son las técnicas adecuadas de balance y corrección en los conjuntos de datos para que no existe un error dentro de esta información que nos está brindando los sistemas de inteligencia artificial.

Sesgos en el diseño algorítmico

> El diseño de algoritmos también puede introducir sesgos. Los errores de programación, como un diseñador de IA que pondera injustamente los factores en el proceso de toma de decisiones, pueden transferirse al sistema sin saberlo. La ponderación suele ser una técnica para evitar sesgos, ya que implica ajustes en los datos para que reflejen mejor la población real. Sin embargo, puede requerir suposiciones por parte de los diseñadores, lo que puede generar imprecisiones e introducir sesgos. Los desarrolladores también pueden integrar el algoritmo con reglas subjetivas basadas en sus propios sesgos conscientes o inconscientes. (Jonker & Julie, 2024)

Dentro de este sistema en el cual el diseño de los algoritmos también puede contribuir al sesgo ya que los desarrolladores pueden introducir decisiones los cuales son de carácter subjetivo y esto no lo pueden hacer de una manera consciente o puede existir la índole de qué este sesgo sea de carácter consciente o inconsciente. Los errores de programación, la ponderación en la propiedad

de ciertos factores incluso de las reglas sesgadas pueden crear resultados parciales es por ello que esta preocupación sobre estos sesgos que son subjetivos de los diseñadores es válida ya que estos algoritmos son creados por personas los cuales tienen una creencia y a su vez tienen una forma de pensar que puede ser distinta al resto de la población es por ello que no existe un pensamiento neutro que puede ser desarrollado por los diseñadores de algoritmos el cual puede tener una conveniencia para todo el público en general.

Este sesgo me parece uno de los más difíciles de controlar debido a que no existe un sistema automatizado o no tengo el conocimiento del mismo en el cual se pueda llegar a brindar una decisión completamente neutra ya que los desarrolladores de los algoritmos son quienes implementan y generan sus ideales dentro de los cuales están expuestos al crear mencionado algoritmo es por ello que es muy difícil de comprender o de generar un punto de quiebre que sea neutral.

Sesgos en los datos proxy

> Los sistemas de IA a veces emplean proxies como sustituto de atributos protegidos, como la raza o el género. Sin embargo, los proxies pueden estar sesgados involuntariamente, ya que podrían tener una correlación falsa o accidental con los atributos confidenciales que debían reemplazar. Por ejemplo, si un algoritmo emplea códigos postales como proxy del estatus económico, podría perjudicar injustamente a ciertos grupos en los que los códigos postales están asociados con datos demográficos raciales específicos. (Jonker & Julie, 2024)

El uso de proxies para atributos sensibles como puede ser la raza o el género es una estrategia común dentro de la inteligencia artificial, pero puede ser un hecho problemático si estos proxies no reflejan con precisión los atributos originales para los cuales fueron desarrollados, debido a que su uso es variable como el código postal para representar el estatus socioeconómico puede introducir sesgos si existe una correlación indirecta con características demográficas lo que lleva decisiones discriminatorias sin que se tenga un factor real es decir sin que se tenga un

conocimiento del mismo que se está efectuando. Este tipo de sesgo yo considero que es sumamente peligroso porque puede ser más difícil de detectar. El uso de proxies puede ser una solución práctica en algunos casos, pero también puede ocultar sesgos subyacentes yo considero que una decisión más adecuada sería utilizar datos que sean explícitamente representativos de los atributos protegidos o tratar de buscar una manera en ajustar los modelos para que las próximos no induzcan sesgos.

Sesgos en la evaluación

> Los sesgos en la evaluación se producen cuando los resultados de los algoritmos se interpretan en función de las ideas preconcebidas de las personas implicadas, y no de los resultados objetivos. Aunque el algoritmo sea neutral y se base en datos, la forma en que una persona o compañía aplique los resultados del algoritmo puede dar lugar a resultados injustos en función de cómo los entienda. (Jonker & Julie, 2024)

Ahora tenemos los sesgos en la evaluación los cuales ocurren cuando los resultados de los algoritmos se interpretan de manera subjetiva o errónea esto es lo que puede dar lugar a una decisión sesgada, incluso si los datos y el algoritmo inciso o neutrales. Este tipo de sesgo considero que es especialmente relevante en el uso de la inteligencia artificial para tomar decisiones sobre individuos, ya que las personas responsables de interpretar los resultados pueden aplicar criterios injustos. Yo considero que este tipo particularmente es un poco insidioso porque puede ocurrir incluso en un sistema diseñado para ser imparcial es decir para ser neutro ya que no se puede tener un conocimiento basto de todo lo que profundiza tener el algoritmo y a su vez la evaluación que se comprende dentro del método que están aplicando los diseñadores. Además, los sistemas de la inteligencia artificial deben ser auditables para garantizar que los resultados no sean malinterpretado o manipulados para justificar decisiones errores o sesgadas.

3.2. Responsabilidad en el tratamiento de datos

3.2.1. ¿Quién responde por los errores cometidos por la IA?

Este es uno de los temas más complicados de nuestra investigación debido a que no se puede dar a conocer un solo culpable ya que son algoritmos los cuales de forma automatizada

brinda esa información, entonces no tenemos un conocimiento previo de quién pudo ser el causante de este daño o de esta vulneración de derechos debido a que no sabemos o no es que no sepamos sino que no se fundamenta en un solo individuo o en alguien a quien a culpar, debido al avance que es de manera muy acelerada de la inteligencia artificial se generan demasiados debates sobre la asignación de responsabilidad cuando estos sistemas lleguen a cometer errores. Ya sabemos que la inteligencia artificial es una de las herramientas fundamentales y muchos sectores claves, desde lo que sería la salud hasta una administración pública, es por ello que se generan interrogantes al no saber quién es el que responde cuando una decisión causa este perjuicio, debido a que estos sistemas no operan de manera aislada, sino que dependen de muchos factores que están antes ya determinados. Por ejemplo es como si estos sistemas ya estuvieran entrenados para dar respuestas automáticas básicamente es como si ya fuera una respuesta de una persona nueva creada de forma tecnológica, si tú le preguntas algo sobre alguna enfermedad te responde, asimismo sobre alguna tarea te responde, entonces se comprende que es como si una máquina hubiera estudiado para dar estas respuestas es por eso que de forma automatizada Según su base de datos genera una controversia ya que es ella es decir la inteligencia artificial quien recrea sus propios respuestas.

Los desarrolladores y fabricantes de IA son los que desempeñan un papel al momento en el cual se crea el sistema, pero la responsabilidad no puede estar de forma clara sobre ellos, obviamente es razonable que respondan por los defectos de la programación o algún tipo de sesgo en los algoritmos, también existen situaciones en las que la responsabilidad podría ser hasta limitada. Por ejemplo, si el sistema ha sido utilizado en el contexto distinto a lo previsto o han sido modificados por terceros la culpa ya no recae sobre el desarrollador, sino que sobre los actores que cambiaron este modelo. Es por ello que necesitamos de una normativa que delimite con precisión hasta dónde llega la responsabilidad de quienes diseña y comercializan estos sistemas.

Al momento en el cual se usa la inteligencia artificial esto no exime a los usuarios finales de toda la responsabilidad, existen muchos casos en los cuales los sistemas se apoyan a la toma de decisiones conjuntamente con el usuario. Si un usuario toma una decisión basada en una recomendación de inteligencia artificial sin validarla adecuadamente, es culpa del mismo. Es decir, no es posible que un doctor el cual ha estudiado varios años para su carrera y para tener conocimiento sobre las enfermedades deba preguntar a una inteligencia artificial qué hacer o qué

enfermedad puede ser, ya que si al preguntar recae un error ya no es culpa del sistema operativo sino del doctor por no tener una respuesta a lo que él debería saber.

Es por ello que una normativa debería limitar hasta donde se da una responsabilidad de una inteligencia artificial basado en un hecho o una toma de decisiones de un usuario sobre algún cierto tema generando una complejidad legal, ya que no existe todavía esta normativa y se debería centrar mucho debido a que la inteligencia artificial es una de las plataformas más utilizadas a nivel mundial. Esto puede traer complicaciones entre los mismos usuarios como mencionamos anteriormente debido a que el humano cada vez se hace más vago y ya no busca por sí mismo, sino que prefiere que una plataforma de inteligencia artificial le dé las respuestas, mismas que pueden ser erróneas y esto puede inducir a que exista algún problema aparte, como el que un abogado pregunte sobre una normativa o sobre un artículo y éste sea erróneo, pero él ya es estipuló el mismo.

3.3. Mitigación de riesgos éticos

3.3.1. Estrategias para un uso ético de IA en la gestión de datos.

Dentro de las estrategias que se debería interpretar e implementar para un uso correcto de la inteligencia artificial en donde no se vulnere una ética y una moral, el primer paso para la implementación de la ética y moral en la inteligencia artificial sería la gestión de datos y a su vez una base que se funde en distintos principios los cuales sirvan de eje fundamental para una guía y desarrollo y a su vez que sean de importante aplicación. Yo considero que una de las claves es la transparencia, esto puesto que permite que los usuarios y partes interesadas o las partes intervienen entes dentro de lo que es la aplicación o sistema puedan llegar a comprender cómo funcionan los algoritmos, los datos que utilizan y cuáles son los criterios empleados en toma de decisiones, es decir cómo se maneja esta tecnología o qué es lo que lleva detrás de la misma. Sin este principio fundamental que es el de la transparencia es muy difícil generar confianza en los sistemas de inteligencia artificial y asimismo se crea una problemática debido a que no sabemos si es que va a existir un uso indebido de la información.

Considero yo que otro de los principios fundamentales que servirían como base es la equidad, puesto que esta implica evitar algún tipo de error o sesgo en los datos y algoritmos mismos que pueden generar discriminación o desigualdad en algún tipo de resultado que arroje. En algunos

momentos o en algunas ocasiones los sistemas de inteligencia artificial reflejan los prejuicios presentes en los datos con los que fueron entrenados, esto es lo que lleva a decisiones injustas en sectores como la selección de personal, la concesión de créditos o el acceso a servicios públicos, estos errores son de índole muy importante debido a que puede generar una vulneración y discriminación hacia ciertos usuarios, para llegar a controlar este riesgo consideramos que es necesario desarrollar técnicas de detección y corrección de sesgos, asimismo debería de fomentarse la diversidad de los equipos de desarrollo, para que no exista un solo punto o una mentalidad, de la cual se base todo el sistema operativo.

Ahora bien, otro de los aspectos fundamentales, si no es por decir, el más importante es el de la privacidad en la gestión de los datos con inteligencia artificial, debido a que los sistemas de inteligencia suelen manejar grandes volúmenes de información personal y privada es crucial aplicar medidas de seguridad como por ejemplo puede ser el cifrado y el control de acceso a los datos. Así podremos controlar quien puede obtener estos datos y quien puede verlos, generando una mayor confianza entre el usuario y el proveedor. Además, considero que es muy importante obtener el consentimiento informado de los usuarios y garantizar que tengan el derecho de conocer, modificar o eliminar su información de los sistemas de inteligencia artificial en el caso de qué no les parezca correcto.

Es por ello que para garantizar un uso ético de la inteligencia artificial es necesario implementar estrategias concretas en diferentes niveles de la organización, es por ello que nuestra tesis se centra en una especie de reforma que se pueda dar para la Ley Orgánica de Protección de Datos Personales. Es por ello que yo considero que de manera crucial se debe dar una reforma a la misma, ya que la inteligencia artificial es un tema nuevo y todavía no se encuentra regularizado debemos de poder enfatizarnos y controlar este sistema de datos, asimismo deberíamos crear ciertas normas y aparte de normas principios de los cuales se va a dar una base y un fundamento para que no se dé, la vulneración de derechos a las personas que utilizan estas ciertas plataformas. El diseño ético de algoritmos también es una estrategia crucial, ya que esto implica que los sistemas de IA deben ser desarrollados considerando múltiples perspectivas y asegurando que no favorezcan a ciertos grupos o a ciertas empresas, ya que debe ser algo que sea neutral para todas las personas las cuales vayan a beneficiarse de estas aplicaciones o sistemas.

3.3.2. El papel de la educación digital en la protección de datos.

Dentro de cualquier parte del mundo, los sistemas tecnológicos son usados de manera cotidiana, en especial en los colegios y escuelas, es por ello que deberíamos tener una educación tecnológica, ya que muchos no conocen lo fuerte del tema, las nuevas tecnologías han cambiado el mundo, ya que con un dispositivo puede hace miles de cosas, es por ello que debemos saber lo que está bien y lo que está mal, y eso nace educando a los jóvenes y niños para que no sufran luego.

> En nuestro mundo digital, la Protección de datos en el sector educativo es cada vez más importante. Los centros escolares procesan diariamente una gran cantidad de información personal de alumnos y profesores. El sitio Protección de datos de los estudiantes para proteger la intimidad de todos los implicados. En Seguridad de los datos educativos no es sólo una obligación legal, sino también una necesidad ética. Los centros escolares deben garantizar que la información sensible esté protegida y solo se utilice para los fines previstos. Este artículo examina diversos aspectos de la protección de datos en los centros escolares. Mostramos cómo los centros educativos pueden garantizar la protección de los datos personales y qué medidas son necesarias para ello. (DATUREX, 2024)

Ahora bien, entendiendo de una mejor manera podemos identificar que la educación digital es uno de los pilares fundamentales en la protección de datos en esta era informática. A medida que el uso de la tecnología y las plataformas digitales se expande y sigue avanzando cada día más y de una forma de descomunal, también lo hacen los riesgos asociados con la privacidad y la seguridad de los datos personales, Esto genera una problemática increíble para las personas que no tengan conocimientos sobre lo que puede llegar a ser un simple móvil o una simple aplicación. Es por eso que la falta de conocimiento sobre cómo gestionar adecuadamente la información digital puede llevar a la exposición de datos sensibles, fraudes y vulneración de privacidad o de intimidad de las personas. Por ello, educar a la población en materia de protección de datos es esencial para garantizar un entorno digital más seguro y consciente.

Uno de los principales aspectos de la educación digital en la protección de los datos es la concientización sobre la importancia de la privacidad en línea. Muchas personas desconocen cómo sus datos son recopilados, utilizados y almacenados por empresas, redes sociales y otras plataformas digitales, a menudo aceptamos lo que son los términos y condiciones sin leerlos proporcionando acceso a información personal sin saberlo, es por eso que también se fomenta una lectura clara y comprensible de lo que vamos a aceptar o firmar.

Yo considero que el papel de los gobiernos en ese aspecto debe ser fundamental, ya que debe ser necesario que las instituciones promuevan campañas de educación digital accesibles para toda la población, con programas específicos para diferentes grupos y sectores, un pueblo o una nación que conoce del tema va a poder luchar contra ciertas amenazas la escuela se le pueden presentar a lo largo de la vida, es por ello que nosotros consideramos que una regulación y a su vez una educación sobre la inteligencia artificial o los sistemas automatizados o la creciente y nueva tecnología que existe dentro de nuestro mundo es una de las bases primordiales para que no existe una vulneración de derechos sobre los mismos.

Capítulo 4: Reforma legal para regular la IA en Ecuador

4.1. Elementos clave para regular la IA

4.1.1. Definición de principios fundamentales para la regulación.

Dentro de nuestro análisis hemos estudiado a los principios los cuales establece la Unesco en el año del 2024 para una regulación de la inteligencia artificial, dentro de este tema se aborda en aspectos fundamentales de esta tecnología desde una perspectiva de los derechos humanos, seguridad y sostenibilidad. En general esta investigación constituye un marco sólido y bien estructurado para guiar el desarrollo y aplicación de la IA a nivel global, es por ello que yo considero que nuestro país debería basarse dentro de lo que sería estos principios para que no existan tantos desafíos y se ponga una limitante a las inteligencias artificiales.

“1. Proporcionalidad e inocuidad el uso de sistemas de IA no debe ir más allá de lo necesario para alcanzar un objetivo legítimo. La evaluación de los riesgos debe utilizarse para prevenir los daños que puedan derivarse de usos ilegítimos.” (UNESCO, 2024)

Este principio nos establece que el uso del área debe ser limitado a lo que sea necesario para alcanzar un objetivo legítimo, también nos dice que enfatiza la importancia de una evaluación de riesgo para prevenir daños derivados de usos individuos, se puede encontrar que este principio evita el uso desproporcionado de la inteligencia artificial en ámbitos donde que no sea realmente necesaria, así establece un control y fomenta una regulación basada en el riesgo lo que permite tomar medidas preventivas antes que ocurren daños

Ahora considero yo, que se debería definir lo que es necesario y también lo que es un objetivo legítimo ya que esta pregunta puede ser un poco subjetiva y variar según el contexto del tema del cual se esté tratando, también en algunos casos de evaluación de riesgo puede volverse un proceso burocrático que ralentice la innovación sin garantizar mejores resultados lo que retro atrae o nos llega a retroceder en el tiempo debido a que ya no se daría un avance sino que vamos a estar estancados dentro de una base.

"2. Seguridad y protección Los daños no deseados (riesgos de seguridad) y las vulnerabilidades a los ataques (riesgos de protección) deberían ser evitados y tomados en consideración." (UNESCO, 2024)

Este principio básicamente tiene su concentración en el que no exista daños no intencionados y en evitar algún tipo de vulneración que pueda ser explotadas por ciber atacantes. La Ciberseguridad es una de las claves las cuales tiene que tener por obligación la inteligencia artificial, especialmente en sistemas críticos como puede ser el de salud, finanzas o defensa ya que estos sistemas deben contar con una seguridad mucho mayor de la de otros sistemas ya que se está tomando un riesgo mucho mayor en el que exista un error o un robo de información, reducir vulnerabilidad evita que la inteligencia artificial sea usada con fines malintencionados. Pero para ello debería existir criterios específicos sobre cómo medir y garantizar la seguridad de un sistema de inteligencia artificial el cual todavía tiene un déficit de criterio. La seguridad puede entrar en conflicto con la transparencia, es decir un sistema más seguro puede ser menos explicable.

"3. Derecho a la intimidad y protección de datos La privacidad debe protegerse y promoverse a lo largo de todo el ciclo de vida de la IA. También deben establecerse marcos adecuados de protección de datos." (UNESCO, 2024)

Este principio nos destaca la necesidad de qué la privacidad se respete en todo ciclo de la vida de la inteligencia artificial, junto con la existencia de marcos adecuados de protección de datos, lo que yo considero que es una de las dejes fundamentales en los cuales se debe centrar la inteligencia artificial debido a que la privacidad y la intimidad son uno de los derechos los cuales pueden ser más vulnerados dentro de la inteligencia artificial como es conocido dentro del ChatGPT el cual nosotros podemos llegar a brindar información que sea de carácter personal con el fin de obtener una respuesta y esta misma se almacena en la base de datos lo cual puede ser robada o alguien puede hackear el sistema para obtener esa información. Se debe proteger a los ciudadanos del uso indebido de sus datos por parte de los sistemas de inteligencia artificial, también se debería alinear con regulaciones existentes como el reglamento general de la protección de datos para que pueda existir una mayor seguridad dentro del mismo. Muchas inteligencias artificiales dependen del acceso a grandes volúmenes de datos, imponer restricciones puede dificultad también su desarrollo entonces esto también es algo subjetivo lo cual no se tiene un conocimiento estricto de lo que puede llegar a pasar ya que al quitar mucha información que puede ser importante para la inteligencia artificial estamos dificultando un desarrollo de la misma pero a su vez también puede existir una vulneración de datos debido al uso excesivo de la información brindada hacia la inteligencia artificial.

> “4. Gobernanza y colaboración adaptativas y de múltiples partes interesadas En el uso de datos, deben respetarse el derecho internacional y la soberanía nacional. La participación de diversas partes interesadas a lo largo del ciclo de vida de los sistemas de IA es necesaria para el desarrollo de enfoques inclusivos de gobernanza.” (UNESCO, 2024)

Aquí se propone que el uso de datos respete la soberanía nacional del derecho internacional promoviendo una participación de distintos actores en la regulación de la IA este es uno de los principios que yo considero que se tiene que tomar en cuenta debido a que la gobernanza inclusiva ayuda a evitar que los grandes corporaciones tecnológicas dicten las reglas y también se respeta a la soberanía de los países en el uso y la regulación de la inteligencia artificiales por eso que

considero que también se debería tomar muy en cuenta ya que éste se va a dar con un limitante para las empresas también.

> "5. Responsabilidad y rendición de cuentas Los sistemas de IA deben ser auditables y trazables. Deben existir mecanismos de supervisión, evaluación de impacto, auditoría y diligencia debida para evitar conflictos con las normas de derechos humanos y amenazas al bienestar medioambiental." (UNESCO, 2024)

En este principio exige que los sistemas de inteligencia artificial sean auditables y trazabas con mecanismos de supervisión y evaluación de impacto ya que así podemos llegar a tener a quien reclamar esto facilita la detección y corrección de errores o sucesos en los algoritmos y también permite a los gobiernos y organizaciones hacer a las empresas tecnologías responsables de sus creaciones, Pero el problema más grande dentro de este principio es que no es siempre es fácil auditar un sistema de inteligencia artificial, especialmente en modelos complejos como los redes neuronales profundas las cuales tienen un sistema automatizado de toma de decisiones, también se podría aumentar los costos de desarrollo y hacer menos accesible la tecnología ya que deberían contar con un mayor índice de seguridad y de qué no exista algún tipo de error o sesgo en lo de algoritmos

> "6. Transparencia y explicabilidad El despliegue ético de los sistemas de IA depende de su transparencia y explicabilidad (T&E). El nivel de T&E debe ser adecuado al contexto, ya que puede haber tensiones entre T&E y otros principios como la privacidad, la seguridad y la protección." (UNESCO, 2024)

Éste principio plantea que los sistemas de inteligencia artificial deben ser comprensibles y explicables, pero también reconoce que esto puede entrar en conflicto con la privacidad y la seguridad es por ello que si aumenta la confianza pública en los sistemas de inteligencia artificial y también permite identificar sesgos y errores en la toma de decisiones automatizadas pero también en algunos modelos de la inteligencia artificial son inherentemente opacos y hacerlos explicables

puede reducir su eficacia y también no hay un estándar único para definir qué tan explicable debe ser un sistema en cada contexto.

"7. Supervisión y decisión humanas Los Estados Miembros deberían velar por que siempre sea posible atribuir la responsabilidad ética y jurídica a personas físicas o a entidades jurídicas existentes." (UNESCO, 2024)

Ahora este principio propone que siempre exista un responsable humano detrás de las decisiones tomadas por inteligencia artificial y si es bueno debido a que evita la toma de decisiones automatizada imposibilidad de la revisión humana y también reduce un riesgo en áreas sensibles como la justicia, la salud y el empleo. Pero en algunos casos la intervención humana puede hacer un proceso más lento debido a que muchas de las personas van a utilizar estos sistemas de inteligencia artificial y deben esperar a que una persona responda por la inteligencia artificial entonces esto se vuelve un proceso ineficiente, la responsabilidad podría diluirse si hay varios actores involucrados en la supervisión de un sistema de inteligencia artificial y no se va a poder tener un conocimiento del mismo.

"8. Sostenibilidad Las tecnologías de IA deben evaluarse en función de su impacto en la "sostenibilidad", entendida como un conjunto de objetivos en constante evolución, incluidos los establecidos en los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas." (UNESCO, 2024)

Este principio sugiere que la inteligencia artificial sea evaluada en función de su impacto ambiental y su contribución a los objetivos de desarrollo sostenible de la ONU así es como se promueve el desarrollo de la inteligencia artificial con menor impacto ecológico y también nos dice que fomenta el uso de la inteligencia artificial para resolver problemas globales como el cambio climático esto es un eje acertado pero también no define cómo medir el impacto ambiental de un sistema de inteligencia artificial y algunas de las guías que requieren gran capacidad de cómputo como por ejemplo puede ser el ChatGPT tienen un alto consumo energético lo que puede dificultar su alineación con los objetivos de desarrollo sostenible.

> "9. Sensibilización y educación La sensibilización y la comprensión del público respecto de la IA y el valor de los datos deberían promoverse mediante una educación abierta y accesible, la participación cívica, las competencias digitales y la capacitación, y la alfabetización mediática e información." (UNESCO, 2024)

En este principio se plantea que la educación y la capacitación en la inteligencia artificial deben ser accesibles para todos los ciudadanos y también es un principio del cual fomenta y mejora la alfabetización digital y ayuda a reducir la brecha de conocimiento en inteligencia artificial así haciendo y permitiendo que más personas participen en la toma de decisiones sobre la inteligencia artificial, pero existe una falta de inversión en educación tecnológico en muchos países y también la rápida evolución de la IA hace difícil mantener los programas educativos actualizados ya que puede que exista una clase o una materia en la cual ya está siendo brindada hacia los estudiantes pero esta tecnología avanza y genera nuevas brechas entonces se debería volver a tomar la clase.

"10. Equidad y no discriminación Los actores de la IA deberían promover la justicia social, salvaguardar la equidad y luchar contra todo tipo de discriminación, adoptando un enfoque inclusivo para garantizar que los beneficios de la IA sean accesibles para todos" (UNESCO, 2024)

El principio de equidad afirma que los desarrolladores de la inteligencia artificial deban garantizar una justicia social y una accesibilidad de la inteligencia artificial para todos evitando así los sesgos discriminatorios debido a que esto es esencial para evitar que los algoritmos perpetúo desigualdades sociales y así también asegura que las personas en situaciones vulnerables se beneficien con los avances de la inteligencia artificial. Pero estos sesgos de la inteligencia artificial pueden ser difíciles de eliminar completamente debido a la naturaleza de los datos utilizados y que se deba profundizar dentro de los datos y el conocimiento más amplio sobre este sesgo también no se establecen mecanismos claros para hacer responsables a las empresas cuando sistemas de IA presenten sesgos es por ello que es uno de los más difíciles de sostener ya que no existe todavía un contrato o un convenio de forma estricta en la cual vincule a una persona o un funcionario en el cual responda por lo que brinda la inteligencia artificial.

4.2. Creación de un ente supervisor para regular la IA.

Dada la creciente implementación de la inteligencia artificial en la gestión y procesamiento de datos, resulta fundamental la creación de un ente supervisor especializado que garantice el uso ético, moral, seguro y transparente de estas tecnologías. Este organismo debe ser encargado de regular, supervisar y auditar el desarrollo y aplicación de la IA en diversos sectores, asegurando que su implementación respete los derechos fundamentales de los ciudadanos y cumpla con la normativa de protección de datos.

Dentro de las funciones las cuales le competía a este ente sería la supervisión y cumplimiento normativo, vigilar la aplicación de la normativa de protección de datos y IA en el sector público y privado sería uno de los ejes fundamentales en las cuales se debe garantizar y a su vez supervisar de manera profunda, ya que garantizar el cumplimiento de principios como transparencia, responsabilidad y equidad en el uso de la inteligencia artificial es uno de los principios y bases que se debe centrar el país para que exista un control sobre la inteligencia artificial. Otra de las funciones sería la auditoría y evaluación de riesgos, ya que al implementar mecanismos de control para evaluar el impacto de la inteligencia artificial en la privación y seguridad de los datos debe ser primordial, y exigir auditorías periódicas de los sistemas de inteligencia artificial, con especial énfasis en aquellos de alto riesgo, para ello también debería existir un control y un sistema de etiquetas las cuales nos indiquen el riesgo de la tecnología. De igual forma este ente debería centrarse en la regulación y actualización normativa, ya que esta tecnología constantemente va cambiando también la normativa debe ir cambiando ya que al avanzar la tecnología también la norma se quedará corta y no comprenderá todo lo nuevo que desarrolló la tecnología, es por ello que propone reformas legislativas que permiten la adopta Sion del marco jurídico a la evaluación de la IA debe ser constante y actuar. La transparencia y aplicabilidad algorítmica debe darse debido a que se busca garantizar que las decisiones automatizadas sean comprensibles y explicables para los ciudadanos, es decir que sea de fácil entendimiento y que las personas puedan comprender y puedan desarrollar de una forma entendible para ellos, y una protección de derechos y educación digital debe ser uno de los puntos más destacables ya que con campañas de concienciación sobre el uso responsable de la IA y la protección de datos facilitará la comprensión y el entendimiento de la gente sobre las tecnologías que van a utilizar o están usando constantemente asimismo se facilitará las herramientas de acceso

y controla los ciudadanos sobre el tratamiento de su información personal así pueden llegar a tener un mayor entendimiento y control sobre los datos que ellos mismos dan a estas tecnologías.

En abril de 2021, la Comisión Europea adoptó la primera respuesta regulatoria con la publicación de la propuesta de Reglamento europeo para la armonización de las normas sobre IA. La propuesta de Reglamento tiene por objetivo establecer los requisitos legales que deben cumplir los sistemas de IA para garantizar los derechos fundamentales frente a los riesgos vinculados a determinados usos de estas tecnologías. Una vez aprobado, será de aplicación directa en todos los Estados Miembros. Tras la aprobación del Parlamento Europeo de su posición sobre la propuesta del Reglamento este pasado 14 de junio de 2023, empezaron las negociaciones institucionales entre los eurodiputados, el Consejo de ministros de la UE y la Comisión conocidas como "trílogos" para la adopción del texto legal final. La aprobación final del Reglamento sobre la IA está prevista para finales de este año, entrando en vigor a finales de 2025. El Reglamento sobre la IA contiene una serie de obligaciones que deben ser asumidas por cada autoridad nacional, motivo por el que España se plantea la creación de una Agencia Estatal, apostando por una supervisión voluntaria de la implementación de estas tecnologías disruptivas, antes de la entrada en vigor de la normativa europea, a través de sellos de calidad y responsabilidad de Inteligencia Artificial, las relaciones con el ecosistema europeo que fomentarán el desarrollo del Pacto por la Inteligencia Artificial, así como el Código de Buenas Prácticas de Inteligencia Artificial Generativa, producido dentro del Consejo de Comercio y Tecnología entre EEUU y la UE. 2. Creación de la AESIA En su artículo único, el Real Decreto crea la AESIA y aprueba su Estatuto. La Agencia será una entidad de derecho público adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificial. Su

> función principal será la de llevar a cabo tareas de supervisión, asesoramiento, concienciación y formación, a empresas públicas y privadas para la adecuada implementación de la normativa entorno al adecuado uso de la IA y concretamente de los algoritmos. Está prevista su efectiva puesta en funcionamiento se producirá con la constitución del Consejo Rector en el plazo máximo de 3 meses desde la entrada en vigor del Real Decreto, es decir, a principios de diciembre de este mismo año. (Monsó & Etxe, 2023)

Al poder revisar la propuesta del reglamento europeo sobre la inteligencia artificial se puede presenciar de un avance muy grande en la regulación de esta tecnología, al establecer un marco armonizado que busca garantizar los derechos fundamentales frente a posibles riesgos, su enfoque basado a animales de riesgo proporciona un marco flexible, pero con exigencias claras para los sistemas de inteligencia artificial de alto impacto.

La dependencia de la AESIA del ministerio de asuntos económicos y transformación digital podría generar inquietudes sobre su autonomía. La independencia de los lentes reguladores es crucial para evitar conflictos de interés entre la supervisión de empresas tecnologías o entidades gubernamentales que emplea en la inteligencia artificial. Sería recomendable establecer garantías que refuerce su imparcialidad y dotarla de recursos suficientes para un monitoreo efectivo. Sin embargo, considero que es un gran avance debido a que con un ente que controle la inteligencia artificial se puede llegar a generar un control y a su vez un desarrollo más amplio de la inteligencia artificial dentro de nuestro estado o de cualquier estado del mundo, es por ello que considero muy inteligente el optar por un ente y un sistema de control que ponga una limitante a la inteligencia artificial para generar un mayor desarrollo a largo plazo y a su vez evitar una problemática sobre la vulneración o discriminación de los derechos de las personas y de los ciudadanos que utilicen estas aplicaciones, a su vez se genera una concientización sobre lo que aborda una inteligencia artificial debido a que tiene una respuesta automática y tienen algoritmos los cuales controlan estas respuestas, es por ello que también saber y conocer más sobre el tema es uno de los ejes fundamentales para poder comprender lo que genera una inteligencia artificial.

Ahora uno de los problemas que yo considero muy importantes es sobre quien recae la culpa en el caso de que exista un problema recurrente sobre algún tipo de inteligencia artificial, existen los desarrolladores y proveedores de los sistemas de inteligencia artificial los cuales son quienes diseñan, entrenan y comercializan sistemas de inteligencia artificial, pero estas personas pueden llegar a ser auditadas por respuestas que son automáticas, o en el caso de empresas o instituciones que implementa la inteligencia artificial como "Chatbots" los cuales almacenan datos que pueden ser de carácter personal serán los responsables de que alguno de estos datos sea vulnerado y esta información pueda llegar a ser robada. Es por ello que considero que la auditoría puede recaer sobre múltiples actores, desde los creadores de la tecnología hasta quién es la usa o supervisa. Esto resulta la importancia de contar con mecanismos claros de responsabilidad de auditoría para garantizar un uso ético y seguro de la inteligencia artificial, y esto debería entrar dentro de lo que es la normativa que se debería proponer a un estado.

4.3. Propuesta de reforma a la LOPDP

Dentro de nuestro enfoque y un análisis, que hicimos dentro de todo nuestra investigación de tesis se debería incorporar una sección específica sobre inteligencia artificial, es decir se debe añadir un capítulo específico dentro de la Ley Orgánica de Protección de Datos Personales que regule el tratamiento de datos personales en los sistemas que utiliza la inteligencia artificial, dentro de esta base y de este capítulo se deberán establecer principios, obligaciones y derechos los cuales son relacionados con la automatización y el aprendizaje de datos. Para esto se debería modificar la Ley Orgánica de Protección de Datos Personales para incluir un título el cual se someta a un control explícito de la inteligencia artificial y la protección de los datos personales, dentro del mismo se definiría los usos permitidos y prohibidos de la inteligencia artificial en el procesamiento de la información personal, asimismo se establecerá mecanismos de control para evitar abusos en la recopilación y análisis de datos por los sistemas automatizados.

Dentro de este capítulo se deberán establecer principios rectores para el uso de la inteligencia artificial en la gestión de datos, ya que la IA utiliza en la gestión de datos debe respetar una serie de principios como ya lo habíamos visto anteriormente se podría basar y sostener en principios de legalidad y finalidad específica. En el uso de inteligencia artificial en el tratamiento de datos personales debe responder a un propósito legítimo, claramente definido y alineado con la normativa de protección de datos, es decir se deberá exigir que todo implementación de

inteligencia artificial en el procesamiento de datos tenga un propósito explícito y documentado, así también se va a prohibir el uso de inteligencia artificial para finalidades no autorizadas o que atente contra los derechos de las personas, asimismo se va a regular la recolección de datos para evitar su explotación sin un consentimiento informado, esto debido a que muchas de las veces la información que se brinda a la inteligencia artificial es información personal o íntima la cual debería necesitar una autorización para guardar dentro de su base de datos para que no pueda existir una vulneración de la misma o una persona conocedora de la informática pueda robar esta información. También se podrá basar en un principio de minimización y proporcionalidad en el cual sólo se podrán procesar los datos personales que sean estrictamente necesarios y proporcionales al objetivo en el cual se lo busco, aquí se va a imponer restricciones a la recopilación masiva de datos mediante inteligencia artificial y obligar a los sistemas de inteligencia artificial que utilicen la menor cantidad de datos posibles ya que muchas de las veces piden datos que no son necesarios y asimismo se implementar criterios de retención de datos para la información innecesaria. Otro principio fundamental sería el de la transparencia y aplicabilidad ya que con este las decisiones tomadas por sistemas de inteligencia artificial deben ser comprensibles, es decir que las personas y los ciudadanos puedan tener un conocimiento y una comprensión de lo que están haciendo y de lo que están dando a conocer, es decir obligar a las empresas a explicar cómo funcionan sus algoritmos y como toman decisiones con los datos que están brindando los ciudadanos. Y una supervisión humana debido a que la toma de decisión automatizadas afecta a derechos fundamentales debe contar con una intervención humana antes de ser ejecutado obviamente este podrá ser un método el cual retrase un poco a la respuesta de la inteligencia artificial, pero se podrá solventar una seguridad en la vulneración de los derechos de las personas.

De igual forma como se mencionó anteriormente un ente supervisor especializado en inteligencia artificial podría ser uno de los propósitos y de los métodos que debe utilizar o que debería utilizar el Estado para que se pueda dar una supervisión de la IA dentro de la Superintendencia de Protección de Datos, el mismo que va a ser encargado de vigilar el uso de la inteligencia artificial en la gestión de los datos personales, se podría crear una oficina especializada con personal capacitado en inteligencia artificial y regulación de datos para que manejen ciertos asuntos los cuales pueden generar una problemática, asimismo se desarrollaría protocolos de auditoría para evaluar el impacto de la inteligencia artificial en la privacidad y también se debería

coordinar con organismos internacionales para alinear la regulación ecuatoriana con estándares globales.

Una regulación de la toma de decisiones automatizadas también se debería implementar dentro de la reforma ya que las personas deben tener derecho a impugnar decisiones tomadas únicamente por inteligencia artificial cuando estas afecten sus derechos ya que así se podrá garantizar que cualquier persona puede exigir una revisión humana de decisiones automatizadas las cuales pudieron haber vulnerado un derecho, así se podría obligar a las empresas a informar a los usuarios cuando una inteligencia artificial interviene en la toma de decisiones, asimismo se implementaría mecanismos de apelación para revisar decisiones automatizadas.

Se debería realizar también evaluaciones de impacto en privacidad para los sistemas de inteligencia artificial ya que toda empresa que implemente inteligencia artificial para tratar datos personales debería realizar una evaluación de impacto en la protección de datos así podríamos mitigar su riesgo, se debería establecer ciertos criterios claros para evaluar riesgos en materia de privacidad y derechos humanos para que no exista una vulneración de la intimidad y así se podrá manifestar una transparencia dentro del proceso, es por ello que estas evaluaciones deberían ser públicas y accesibles a las autoridades de control.

También debería existir sanciones las cuales deberían ser específicas en el uso de la inteligencia artificial en gestión de datos, obviamente este uso debe ser ilegal, ilegítimo o indebido, así se podrán establecer sanciones según la gravedad del uso indebido de la inteligencia artificial, las mismas que se van a clasificar en leves graves y muy graves con multas progresivas y sanciones progresivas, también se podrán establecer sanciones por falta de transparencia, discriminación algorítmica o un uso ilegal de datos y así permitir la inhabilitación de empresas que no cumplan con una normativa para que ya no exista una vulneración de los derechos humanos.

CONCLUSIÓN

La presente investigación sobre la reforma a la Ley Orgánica de Protección de Datos para integrar el uso y control de la inteligencia artificial en la gestión y procesamiento de datos nos ha permitido identificar los principales desafíos y oportunidades que presenta la regulación en este ámbito. A lo largo del estudio y el análisis se ha logrado investigar y se han abordado aspectos esenciales relacionados con la protección de datos personales, el impacto de la inteligencia

artificial en la privacidad y los derechos de los ciudadanos, así como la necesidad de un marco normativo que garantiza un equilibrio entre la innovación tecnológica y la seguridad jurídica.

Uno de los hallazgos más relevantes es que la legislación actúa en Ecuador presenta varios vacíos normativos en cuanto al reglamento de datos, debido a que todavía no existe una normativa que regula y controle la inteligencia artificial. La rápida evolución de estas tecnologías ha superado la capacidad de adaptación de las leyes vigentes, lo que genera un escenario en el que se hace indispensable una renovación y actualización normativa que contemple los principios de transparencia, responsabilidad y control ciudadano sobre los datos personales privados e íntimos. En este sentido se concluye que la reforma a la LOPDP debe priorizar la implementación de mecanismos que permiten una supervisión efectiva del uso de inteligencia artificial en la gestión de la información, evitando abusos y garantizando la protección de los derechos fundamentales, esto con el fin de dar una seguridad y garantizar un cumplimiento con los principios éticos y morales que debe tener y que se debe regir un estado.

De igual forma se han evidenciado que la implementación de la inteligencia artificial en el procesamiento de datos ofrece múltiples beneficios, como la optimización de procesos, la reducción de errores y la mejora en la toma de decisiones. Pero esto no sólo viene cargado de beneficios sino también cargado de riesgos, Tales como la discriminación algorítmica, falta de explicación en los sistemas automatizados y la posible vulneración de la privacidad de los ciudadanos. Por lo mismo, la reforma legal debe establecer parámetros claros para la auditoría y supervisión de los sistemas de inteligencia artificial, asegurando que su uso sea ético, transparente y de acuerdo con los derechos humanos.

Un aspecto fundamental identificado en la investigación es la importancia de la cooperación entre el sector público, privado y la sociedad civil en la formulación de políticas que regulan el uso de la inteligencia artificial en la gestión y procesamiento de datos. La participación de expertos en tecnología, derecho y ética resulta clave para garantizar que la normativa contemple todas las dimensiones necesarias para una regulación efectiva, ya que esta inteligencia artificial tiene un control o una toma de decisiones de automatizada, es como si estuviéramos tratando con una persona y no con una máquina, en este sentido se debería de tomar en cuenta no sólo un criterio sino el criterio de varias personas para llegar a una regulación y control.

También se han observado que varios países han adoptado medidas avanzadas para regular el uso de inteligencia artificial en el tratamiento de datos personales, entre los cuales el que más destaca es el de la unión europea, los cuales deberían de servir como referencia para establecer normativas que promuevan el equilibrio entre el desarrollo tecnológico y la protección de la privacidad, nuestro país puede beneficiarse de estas políticas que se encuentran establecidas y crear una reforma para nosotros los ciudadanos.

La capacitación y el fomento de la lectura y aprendizaje, tanto como el de la educación digital deberían ser temas que a considerar son muy primordiales, y se debería establecer dentro de toda la nación para que así la gente pueda llegar a entender un poco más sobre esta tecnología tan innovadora y tan progresista, ya que esta tecnología cuenta con elementos y diseños que cada día se actualizan también se debería actualizar la educación y precautelar o fomentar el uso de la lectura para tener más conocimiento sobre lo que nosotros mismo aceptamos y nos beneficiamos de ello. Debido a que no tenemos un conocimiento claro de estas nuevas tecnologías es que nosotros no avanzamos y nos estancamos en un solo punto, la ciudadanos son los que aceptan los términos y condiciones que impone una máquina o una aplicación, muchas de las personas ni siquiera leen lo que aceptan al momento en el cual leen los términos y condiciones, es por ello que con el fomento de una educación y el fomento de la lectura, se puede mejorar esta situación que puede llegar a generar riesgos ya que aceptan que aplicaciones puedan utilizar su información personal. Es por ello que al lograr crear una normativa que rija estos términos y estas condiciones podemos llegar a fomentar un pueblo que esté lleno de seguridad jurídica, de seguridad social y de una seguridad informática.

La reforma a la LOPDP en Ecuador no sólo representa una necesidad jurídica, sino también una oportunidad para posicionar al país a la vanguardia en términos de protección de datos y uso responsable de la inteligencia artificial. La implementación de políticas claras, la cooperación entre distintos sectores y la educación digital son los pilares fundamentales que pueden llegar y hacer que nuestro país avance y logre un marco normativo que equilibre la innovación tecnológica con la seguridad y el respeto a los derechos fundamentales que nosotros como ciudadanos en el momento en el cual llegamos a estar dentro de nuestro Estado debemos tener y este derecho se debe respetar. Con estas bases, Ecuador puede avanzar a un futuro en el que la inteligencia artificial sea una aliada del desarrollo y el bienestar social, garantizando al

mismo tiempo el respeto a la privacidad y la seguridad de la información de todos los ciudadanos.

BIBLIOGRAFIA

Datos Personales Protegidos. (2022). Entendiendo la proteccion de datos en el Ecuador: Una guía completa. *Datos personales protegidos*. Obtenido de https://datospersonalesprotegidos.puntanetwork.com/regulaciones-latinoamericanas/entendiendo-ley-proteccion-datos-ecuador-guia-completa/

DATOS PERSONALES PROTEGIDOS. (2022). PERSONAS JURIDICAS. *DATOS PERSONALES PROTEGIDOS*. Obtenido de https://datospersonalesprotegidos.puntanetwork.com/

DATOS PERSONALES PROTEGIDOS. (2022). PERSONAS NATURALES. *DATOS PERSONALES PROTEGIDOS*. Obtenido de https://datospersonalesprotegidos.puntanetwork.com/regulaciones-latinoamericanas/entendiendo-ley-proteccion-datos-ecuador-guia-completa/

DATUREX. (2024). Protección de datos en la educación: proteger los datos de alumnos y profesores. *DATUREX*. Obtenido de https://externer-datenschutzbeauftragter-dresden.de/es/proteccion-de-datos/proteccion-de-datos-en-la-ensenanza-proteccion-de-datos-de-alumnos-y-profesores

ESPAÑA DIGITAL. (2024). Entra en vigor el Reglamento de Inteligencia Artificial de la Unión Europea. *ESPAÑA DIGITAL*. Obtenido de https://espanadigital.gob.es/actualidad/entra-en-vigor-el-reglamento-de-inteligencia-artificial-de-la-union-europea

GDPR. (2018). ART. 22. *GDPR*. Obtenido de https://gdpr-info.eu/

GDPR. (2018). ART. 32. *GDPR*. Obtenido de https://gdpr-info.eu/art-32-gdpr/

GDPR. (2018). Art. 35. *GDPR*. Obtenido de https://gdpr-info.eu/art-35-gdpr/

GDPR. (2018). ART. 5. *GDPR*. Obtenido de https://gdpr-info.eu/art-5-gdpr/

GDPR. (2018). ART. 6. *GDPR*. Obtenido de https://gdpr-info.eu/art-6-gdpr/

Ibañez, M. (2024). La IA generativa trabaja con estadística, no puede hacer arte": dibujantes, guionistas y actores de doblaje exigen más control en su uso y que no los sustituya. *CADENA SER*. Obtenido de https://cadenaser.com/nacional/2025/03/16/la-ia-generativa-trabaja-con-estadistica-no-puede-hacer-arte-dibujantes-guionistas-y-actores-de-doblaje-exigen-mas-control-en-su-uso-y-que-no-los-sustituya-cadena-ser/

Jonker, A., & Julie, R. (2024). ¿Qué es el sesgo algorítmico? *IBM*. Obtenido de https://www.ibm.com/mx-es/think/topics/algorithmic-bias

Ley Orgánica de Protección de Datos Personales. (2021). Registro Oficial Suplemento No. 459 de 26 de mayo de 2021. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

LOPDP. (2022). ARTICULO 8. *LOPDP*. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Luis Enrique Velasco. (2024). la era dorada de las redes sociales toca su fin: la regulacion esta vez va enserio. *El País*. Obtenido de https://elpais.com/proyecto-tendencias/2024-10-

09/la-era-dorada-de-las-redes-sociales-toca-su-fin-la-regulacion-esta-vez-va-en-serio.html

Mendez, J. (2025). BRASIL: EL SENADO APRUEBA EL PROYECTO DE LEY 2338-2023 SOBRE EL USO DE LA IA. *INSTITUTO AUTOR*. Obtenido de https://institutoautor.org/el-senado-de-brasil-aprueba-el-proyecto-de-ley-2338-2023-sobre-el-uso-de-la-inteligencia-artificial

Monsó, P., & Etxe, L. (2023). La nueva Agencia Española de Supervisión de Inteligencia Artificial. *PERISCOPIO FISCAL Y LEGAL*. Obtenido de https://periscopiofiscalylegal.pwc.es/la-nueva-agencia-espanola-de-supervision-de-inteligencia-artificial/

Rodríguez Almache, E. L. (2024). Implementación y desafíos de los principios de la Ley Orgánica de Protección de Datos Personales en Ecuador, Un enfoque de revisión sistemática. *Pro Sciences: Revista De Producción, Ciencias E Investigación*, 48. Obtenido de https://journalprosciences.com/index.php/ps/article/view/753/803

RTVE. (2023). El Gobierno aprueba el estatuto de la Agencia Española de Supervisión de la Inteligencia Artificial. *RTVE*. Obtenido de https://www.rtve.es/noticias/20230822/gobierno-aprueba-agencia-espanola-supervision-inteligencia-artificial-espana/2454434.shtml

UNESCO. (2024). Ética de la inteligencia artificial. *UNESCO*. Obtenido de https://www.unesco.org/es/artificial-intelligence/recommendation-ethics

ANEXOS

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Christian Adrian Criollo Vera, portador(a) de la cédula de ciudadanía **N.º 0105755185**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Reforma a la ley de datos para integrar el uso y control de IA en la gestión y procesamiento de datos"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, 22 de mayo de 2025

F: .....

Christian Adrian Criollo Vera

C.I. **0105755185**