UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TEMA:

Impacto de la inteligencia artificial en la privacidad y seguridad en la era digital

AUTORAS:

Morales Tambo, Jessica Anabel

Parrales Aveiga, Andrea Michelle

Trabajo de titulación previo a la obtención del grado de

ABOGADA

TUTOR:

Abg. García Auz, José Miguel, Mgs.

Guayaquil, Ecuador

23 de abril del 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Morales Tambo, Jessica Anabel y Parrales Aveiga, Andrea Michelle,** como requerimiento para la obtención del Título de **Abogada**.

TUTOR

f. 

Abg. García Auz, José Miguel, Mgs.

DIRECTORA DE LA CARRERA

f. _____

Dra. Pérez Puig-Mir, Nuria, PhD

Guayaquil, a los 23 días del mes de abril del año 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotras, **Morales Tambo, Jessica Anabel y Parrales Aveiga, Andrea Michelle**

DECLARAMOS QUE:

El Trabajo de Titulación: **Impacto de la Inteligencia Artificial en la Privacidad y Seguridad en la Era Digital**, previo a la obtención del título de Abogada, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 23 días del mes de abril del año 2024

LAS AUTORAS

f. _____

Morales Tambo, Jessica Anabel

f. _____

Parrales Aveiga, Andrea Michelle

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Nosotras, **Morales Tambo, Jessica Anabel y Parrales Aveiga, Andrea Michelle**

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación, **Impacto de la Inteligencia Artificial en la Privacidad y Seguridad en la Era Digital,** cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 23 días del mes de abril del año 2024

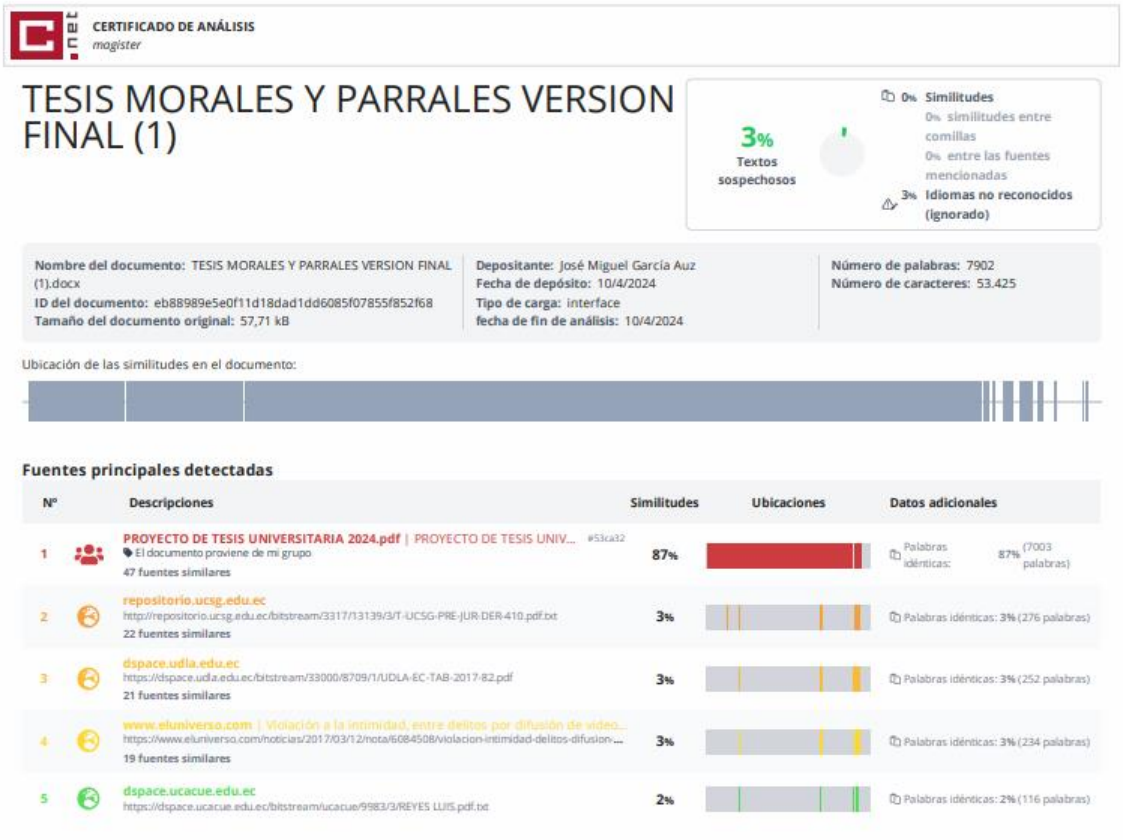
LAS AUTORAS

f. _____
Morales Tambo, Jessica Anabel

f. _____
Parrales Aveiga, Andrea Michelle

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS
CARRERA DE DERECHO
REPORTE



CERTIFICADO DE ANÁLISIS
magister

TESIS MORALES Y PARRALES VERSION FINAL (1)

3% Textos sospechosos

0% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
3% Idiomas no reconocidos (ignorado)

Nombre del documento: TESIS MORALES Y PARRALES VERSION FINAL (1).docx
ID del documento: eb88989e5e0f11d18dad1dd6085f07855f852f68
Tamaño del documento original: 57,71 kB

Depositante: José Miguel García Auz
Fecha de depósito: 10/4/2024
Tipo de carga: interface
fecha de fin de análisis: 10/4/2024

Número de palabras: 7902
Número de caracteres: 53.425

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	PROYECTO DE TESIS UNIVERSITARIA 2024.pdf | PROYECTO DE TESIS UNIV... #53ca32 El documento proviene de mi grupo 47 fuentes similares	87%		Palabras idénticas: 87% (7003 palabras)
2	repositorio.ucsg.edu.ec http://repositorio.ucsg.edu.ec/bitstream/3317/13139/3/T-UCSG-PRE-JUR-DER-410.pdf.txt 22 fuentes similares	3%		Palabras idénticas: 3% (276 palabras)
3	dspace.udla.edu.ec https://dspace.udla.edu.ec/bitstream/33000/8709/1/UDLA-EC-TAB-2017-82.pdf 21 fuentes similares	3%		Palabras idénticas: 3% (252 palabras)
4	www.eluniverso.com | Violación a la intimidad, entre delitos por difusión de video... https://www.eluniverso.com/noticias/2017/03/12/nota/6084508/violacion-intimidad-delitos-difusion-... 19 fuentes similares	3%		Palabras idénticas: 3% (234 palabras)
5	dspace.ucacue.edu.ec https://dspace.ucacue.edu.ec/bitstream/ucacue/9983/3/REYES LUIS.pdf.txt	2%		Palabras idénticas: 2% (116 palabras)

LAS AUTORAS

f. _____
Morales Tambo, Jessica Anabel

f. _____
Parrales Aveiga, Andrea Michelle

TUTOR

Firmado electrónicamente por:
JOSE MIGUEL GARCIA AUZ

f. _____

Abg. García Auz, José Miguel, Mgs.

AGRADECIMIENTO

A Dios, por concederme la bendición de vivir esta experiencia que se llama vida.

A mi padre, Víctor Hugo Parrales Aragones, por su inquebrantable apoyo, esfuerzo y dedicación, sin los cuales este logro no habría sido posible. Papá, tu sacrificio desinteresado ha sido la luz que ha guiado mis pasos, y lo llevaré por siempre grabado en mi corazón y memoria.

A mi madre, Jenny del Rocío Aveiga Delgado, quien es la fuerza impulsora que me motiva a ser la mejor versión de mí misma. Mamá, gracias por tu infinito apoyo, y por desear siempre lo mejor para mí. Quedará grabado en mi corazón y memoria todo el sacrificio que hiciste para que yo pudiera brillar.

A mi querida hermanita, María Paula, quien entró como un rayo de luz y esperanza a mi vida. Tu constante cariño y amor han llenado mi mundo de colores y alegría.

A mi linda hermanita, Valentina, quien siempre me ha estado ayudando y apoyando constantemente.

A mi hermano Andrés, por ser mi primer amigo, y ser alguien confiable.

A mi abuelita, María Italia Delgado Vega, quien fue un ángel terrenal que guardo con cariño en mi corazón.

A mi abuelita Julia Betty Aragones Lucero, en la admirable figura de mi padre veo reflejado tu esfuerzo y dedicación.

A mi compañera de tesis, Jessica Morales Tambo, quien me apoyó en este proceso y juntas logramos crear un trabajo del que estamos orgullosas. Jess, lo logramos.

A Tommy, el pequeño sol que iluminó mi universo, y a quien recuerdo cada día con mucho amor.

DEDICATORIA

A mi familia, mi pilar fundamental en la vida. Gracias por ser mi red de apoyo incondicional, por sus palabras de aliento, por sus consejos oportunos y por celebrar cada uno de mis logros. Son el tesoro más preciado que tengo, y me siento inmensamente afortunada de tenerlos en mi vida. Doy dos veces gracias.

- Andrea Michelle Parrales Aveiga

AGRADECIMIENTO

En este presente trabajo, en primer lugar, agradezco a Dios por iluminar mi camino con valiosas enseñanzas.

Mi entera gratitud a mis amados padres, Carlos Eduardo Morales Almeida y Emma Marisol Tambo Tungui, su inquebrantable determinación, sabiduría y amor. Con su constante apoyo, fortaleza y valentía, han sabido guiarme en mi crecimiento personal, dejando en cada enseñanza la bondad, generosidad y una cálida sonrisa. Su invaluable amor, paciencia y comprensión son un ejemplo que siempre me inspirará. Su sacrificio silencioso y entrega desinteresada han dejado una marca indeleble en mi corazón.

Mi estima a mi querida hermana mayor, Katty Estefanía Morales Tambo, agradezco tanto por tu presencia constante en mi vida, por ser mi cómplice de travesuras, siempre cuidando de mí, aconsejándome e impartiéndome tus experiencias. A la vez nombro a mi sobrino querido, tienes una parte de mi amor y ese cariño que siento por ti, siempre prevalecerá.

Mención a mi preciada amiga y compañera de tesis, Andrea Parrales, una amistad de la cual estoy orgullosa de tener, gracias por siempre escucharme y aconsejarme.

Por último, pero no menos importante, a Max el amor de mi vida en mascota, fuiste el ser más lindo y puro que pudo llegar a mi vida cuando más lo necesitaba, te recuerdo todos los días con mucho amor y nostalgia, porque contigo se fue una parte de mi corazón, aun así, sé que desde donde estés siempre me cuidarás.

Gracias por esta aventura llamada vida.

DEDICATORIA

Esta meta cumplida se la dedico a mi familia quienes son mis mayores ejemplos a seguir, mis amigas que me han brindado su apoyo y seres queridos que han pasado por mi vida, cada uno dejando una marca imborrable. Pueden presentarse momentos en los que podemos sentir el mundo caérsenos encima, pero como dice Shawn Mendes en su canción: “It’ll be Okay”.

- Jessica Anabel Morales Tambo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

Dr. Zavala Egas, Leopoldo Xavier, Mgs.

DECANO

f. _____

Ab. Reynoso Gaute, Maritza Ginette, Mgs.

COORDINADORA DEL ÁREA

f. _____

OPONENTE

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: Jurisprudencia

Carrera: Derecho

Periodo: SEMESTRE C 2024

Fecha: 21/04/2024

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado ***Impacto de la Inteligencia Artificial en la Privacidad y Seguridad en la Era Digital*****,** elaborado por las estudiantes ***Morales Tambo, Jessica Anabel y Parrales Aveiga, Andrea Michelle,*** certifica que durante el proceso de acompañamiento dichas estudiantes han obtenido la calificación de **10 (DIEZ)**, lo cual las califica como **APTAS PARA LA SUSTENTACIÓN.**

Firmado electrónicamente por:
JOSE MIGUEL
GARCIA AUZ

Abg. García Auz, José Miguel, Mgs.

INDICE

RESUMEN

En el escenario jurídico de Ecuador, la intersección entre la protección de datos y la cada vez más extendida implementación de sistemas de Inteligencia Artificial (IA) presenta una red de desafíos que se entrelazan en una compleja ambigüedad normativa. Esta investigación, respaldada por un enfoque interdisciplinario que amalgama análisis jurídicos y tecnológicos, se sumerge en esta intrincada maraña para no solo comprender, sino también resolver, la incertidumbre que surge al aplicar las regulaciones de protección de datos a la IA. El examen exhaustivo aborda la esencia misma, los orígenes y las ramificaciones de esta ambigüedad, con un énfasis particular en los desafíos asociados a la asignación de responsabilidades y a la preservación de la privacidad.

El presente estudio no se limita a una mera exploración superficial; por el contrario, se adentra en una investigación minuciosa y detallada, con el foco puesto en identificar y abordar los desafíos complejos que emergen en este cruce entre el ámbito jurídico y tecnológico. Su propósito es ofrecer soluciones concretas y efectivas que puedan moldear el panorama normativo del país, específicamente en la era desafiante y fascinante de la Inteligencia Artificial.

Palabras claves: Sistemas de Inteligencia Artificial (IA), Base de datos, Protección de datos personales, Consentimiento, Privacidad Digital, DeepFakes, Combinar, Fusionar, Sustituir, Simular

ABSTRACT

In the legal landscape of Ecuador, the intersection between data protection and the increasingly widespread implementation of Artificial Intelligence (AI) systems presents a network of challenges interwoven in a complex normative ambiguity. This research, supported by an interdisciplinary approach that blends legal and technological analyses, delves into this intricate web to not only comprehend but also resolve the uncertainty that arises when applying data protection regulations to AI. The comprehensive examination addresses the very essence, origins, and ramifications of this ambiguity, with a particular emphasis on challenges associated with responsibility assignment and privacy preservation.

This study goes beyond a mere surface exploration; instead, it undertakes a meticulous and detailed investigation, focusing on identifying and addressing the complex challenges that emerge at the intersection of legal and technological realms. Its purpose is to provide concrete and effective solutions that can shape the regulatory landscape of the country, specifically in the challenging and fascinating era of Artificial Intelligence.

Keywords: Artificial Intelligence (AI) Systems, Database, Personal data Protection, Consent, Digital Privacy, Deepfake, Combine, Merge, Replace, Simulate

INTRODUCCIÓN

En el vasto horizonte jurídico de Ecuador, el dinámico cruce entre la salvaguarda de datos personales y la progresiva implementación de Sistema de Inteligencia Artificial (IA) genera una confluencia compleja y desafiante que exige un análisis minucioso y una comprensión integral. Este complejo tejido normativo, donde se entrelazan las disposiciones sobre protección de datos con el vertiginoso avance de la IA, ha engendrado un terreno fértil para el vacío, generando un desafío sustancial en la aplicación efectiva de la legislación existente. La presente investigación surge como respuesta a este llamado, adoptando una aproximación multidisciplinaria que fusiona las esferas del derecho y la tecnología.

Dentro de este viaje intelectual, nos enfocamos en un análisis detallado y exhaustivo, explorando la esencia misma del vacío normativo, explayando sus raíces y explorando las múltiples ramificaciones que desprende este entramado legal y tecnológico. Ante el rápido avance de los medios digitales e inteligencia artificial podemos encontrar un inminente peligro latente al compartir y consumir información de datos personales, ya que esto no sólo concluye aquellos términos, sino que a su vez pueden combinar, fusionar, sustituir y simular, todo ello englobado en el intercambio de rostros, especialmente en imágenes y vídeos, o la manipulación de la expresión facial que se denominan métodos Deepfake. “Describe la capacidad de usar Inteligencia Artificial (IA) para falsificar las caras de personas con aún más facilidad” (Daus, 2019). Este tipo de contenido es actualmente considerado un instrumento de acoso que promueve el conflicto en la sociedad, a través de la creación de materiales audiovisuales fraudulentos sin el consentimiento del individuo a quien imitan, vulnerando así el derecho a la privacidad, y de igual manera al derecho de intimidad, honor y propia imagen.

Con base a todo lo anteriormente explicado, el presente trabajo busca abordar la compleja intersección entre la falta de contenido de la protección de datos personales y el extenso uso de la Inteligencia Artificial (IA) en el Ecuador. Focalizándose en un análisis generado a causa de ello por la conectividad normativa y tecnológica adoptando una aproximación multidisciplinaria que fusiona el derecho y la tecnología. Del mismo modo en el que se explora a detalle el fenómeno Deepfake y su gran conmoción en la transgresión hacia derechos personales que son irrenunciables, todo con el objetivo de ser capaces de comprender y abordar los altos riesgos de proporcionar y adquirir información de datos personales en un escenario donde las herramientas digitales siguen en una incesante evolución.

CAPÍTULO I

I. Antecedentes histórico jurídico

La protección de los datos personales se encuentra consagrada como un derecho fundamental en la **Constitución de la República del Ecuador** de 2008. En su artículo 66, numeral 19, se establece claramente el reconocimiento y garantía de *"el derecho a la protección de datos de carácter personal"* (2008, pág. 33)., la cual abarca no solo el acceso y la capacidad de decisión sobre la información y datos de esta índole, sino también su salvaguardia correspondiente. Según lo estipulado, la recolección, archivo, procesamiento, distribución o divulgación de dichos datos o información deben contar con la autorización expresa del titular o estar respaldados según lo establecido en la ley. En el mismo artículo, numeral 20, se reconoce y garantiza el derecho a la intimidad personal y familiar.

En el año 2021, la Asamblea Nacional aprobó la Ley Orgánica de Protección de Datos Personales, a continuación, como LOPD, con 118 votos afirmativos. La ley fue impulsada por una serie de factores, entre ellos el creciente uso de las tecnologías de la información y la comunicación, que han incrementado el riesgo de que los datos personales sean vulnerados.

La LOPD tiene como objetivo garantizar el derecho de las personas a la protección de sus datos personales, así como a su adecuada utilización. La ley establece un marco regulatorio para el tratamiento de datos personales, que incluye principios, derechos y obligaciones para los responsables y encargados del tratamiento.

"La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior" (Ley Orgánica de Protección de Datos, 2021, 26 de mayo). A diferencia de los sistemas automatizados convencionales, los sistemas automatizados con IA pueden tomar decisiones sobre las personas sin su consentimiento o conocimiento, lo que puede vulnerar el principio de licitud y el principio de transparencia.

La LOPD, concebida en un periodo anterior al auge significativo de la IA, no abordaba directamente esta vertiginosa evolución tecnológica en su formulación original. Sin embargo, sus principios fundamentales poseen resonancias intrínsecas y pautas aplicables que encuentran eco en el universo de la IA. Principios como el consentimiento informado para el tratamiento de datos personales, la minimización de la cantidad de datos recopilados, la garantía de seguridad y confidencialidad en el manejo de información, y la transparencia en el uso de datos, sientan los cimientos éticos y jurídicos que repercuten en el contexto de la IA.

La actual irrupción de la IA en diversos ámbitos plantea desafíos complejos, donde la LOPD puede fungir como marco conceptual para reflexionar sobre las intersecciones y dilemas emergentes. La necesidad de adaptar y complementar la legislación vigente para abordar específicamente las complejidades de la IA en relación con la protección de datos se vuelve imperativa. Aspectos como la responsabilidad inherente al tratamiento de datos por sistemas automatizados, la exigencia de aplicabilidad en las decisiones algorítmicas, la minimización de riesgos asociados a la utilización de algoritmos, y la preservación rigurosa de los derechos individuales, emergen como prioridades inaplazables.

La LOPD, si bien concebida en un contexto diferente, sienta las bases legales y éticas que podrían adaptarse y enriquecerse para abordar los retos y oportunidades presentes en la era de la IA. Su evolución y adaptación constante resultan críticas para garantizar un marco normativo actualizado, eficiente y sensible a las complejidades inherentes a la protección de la privacidad en el dinámico escenario que dibuja la Inteligencia Artificial en el contexto jurídico de Ecuador.

El Código Orgánico Integral Penal tipifica en el Art. 178 el delito de violación a la intimidad. Este delito se configura cuando una persona accede, intercepta, examina, retiene, graba, reproduce, difunde o publica datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona sin su consentimiento o autorización legal.

No obstante, el presente artículo no regula la creación, distribución, edición, retención, difusión de audios o vídeos creados por inteligencia artificial.

1. Definiciones

A. Inteligencia Artificial

La Inteligencia Artificial (IA), es comprendida como "un campo de la informática que se enfoca en crear sistemas que puedan realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción" (Plan de Recuperación, Transformación y Resiliencia, 2023). Asimismo, estas herramientas digitales tienen la capacidad para aprender nuevo contenido, razonar y ejecutar acciones que precisan de la inteligencia del ser humano. En el contexto legal se define como un conjunto de tecnologías y algoritmos que buscan emular y ejecutar tareas cognitivas propias de la inteligencia humana, con el fin de analizar datos, tomar decisiones y realizar acciones específicas. Desde una perspectiva legal, la IA plantea desafíos y oportunidades significativos, ya que su aplicación abarca áreas como la privacidad, la responsabilidad, la equidad y la transparencia.

En términos legales, la inteligencia artificial involucra la creación y utilización de sistemas autónomos o semiautónomos capaces de procesar grandes volúmenes de información, adaptarse a patrones cambiantes y realizar acciones autónomas. Este campo legal aborda cuestiones fundamentales, como la asignación de responsabilidades en casos de decisiones automatizadas, la protección de datos personales en entornos impulsados por algoritmos, y la garantía de equidad y transparencia en los procesos automatizados. Además, la IA plantea interrogantes éticas y legales relacionadas con la propiedad intelectual, la seguridad cibernética y la posible discriminación algorítmica. A medida que la inteligencia artificial se integra en diversos sectores, desde la atención médica hasta la toma de decisiones gubernamentales, el marco legal busca evolucionar para abordar de manera efectiva estos desafíos, asegurando la protección de derechos fundamentales y promoviendo la responsabilidad en el desarrollo y uso de estas tecnologías.

B. Base de Datos

Una base de datos en el ámbito tecnológico y jurídico es un conjunto organizado de información almacenada electrónicamente que se relaciona con aspectos legales y tecnológicos. Esta base de datos puede contener información sobre leyes, regulaciones, casos judiciales, precedentes legales, así como también datos relacionados con la tecnología, como patentes, derechos de autor, contratos digitales, entre otros.

En el ámbito jurídico, una base de datos puede ser utilizada para gestionar información legal, realizar investigaciones jurídicas, seguir casos judiciales, y proporcionar acceso eficiente a la legislación y jurisprudencia relevante. En el ámbito tecnológico, puede abordar cuestiones relacionadas con la protección de derechos de propiedad intelectual, normativas de privacidad, ciberseguridad, contratos tecnológicos y otros aspectos legales vinculados a la tecnología.

"Las bases de datos son la piedra angular de la documentación jurídica. Estas han sido una revolución en la busca y acceso a la documentación" (Mestre, 2020). Esta integración de la tecnología y la ley en una base de datos facilita la gestión eficiente de información crítica para profesionales del derecho, tecnólogos y otras partes interesadas, contribuyendo a una toma de decisiones informada y cumplimiento normativo.

C. Protección de Datos Personales

La protección de datos personales se refiere al conjunto de medidas, prácticas y regulaciones destinadas a preservar la privacidad, confidencialidad e integridad de la información que identifica a individuos. Este campo aborda cómo las organizaciones y entidades tratan, almacenan, procesan y comparten los datos personales, asegurando que se realice de manera ética, transparente y en conformidad con las leyes y regulaciones pertinentes.

Los principios fundamentales de la protección de datos personales incluyen la necesidad de obtener el consentimiento informado antes de recopilar o procesar datos, la limitación del uso de la información a propósitos específicos, la garantía de la exactitud de los datos y la implementación de medidas de seguridad para prevenir accesos no autorizados o divulgaciones indebidas.

D. Consentimiento

En el ámbito legal, el consentimiento es un principio fundamental en la protección de datos personales. Se define como la autorización voluntaria y específica que otorga un individuo para que sus datos personales sean recopilados, procesados y utilizados por una entidad u organización con fines previamente definidos. En el contexto de la protección de datos, se encuentra detallada en su ley en el Art. 4 lo siguiente: "Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos" (2021, pág. 6).

El consentimiento debe ser informado, lo que implica que la persona debe recibir información clara y comprensible sobre cómo se utilizarán sus datos antes de dar su aprobación. Además, debe ser libre, es decir, sin presiones ni coerciones que puedan afectar la decisión del individuo.

Este actúa como un mecanismo crucial para empoderar a los individuos, brindándoles control sobre cómo se manejan sus datos personales y asegurando que las entidades que recopilan información lo hagan de manera ética y transparente. La falta de consentimiento adecuado puede tener implicaciones legales significativas, destacando la importancia de su obtención correcta y documentada.

E. Privacidad Digital

"La privacidad digital se define como el grado de control que posee un usuario de Internet sobre sus datos personales, pudiendo elegir cuáles datos comparte y cuáles no, así como limitar el acceso de otras personas o instituciones a estos" (Santos, 2024). La privacidad digital, en el contexto contemporáneo, abarca un espectro complejo de preocupaciones y consideraciones que se entrelazan con la evolución constante de la tecnología y la creciente interconexión en línea. Este concepto se refiere al derecho inherente de los individuos a gestionar, controlar y resguardar su información personal en un

entorno digital que se caracteriza por la rápida recopilación, procesamiento y compartición de datos.

En la era digital, nuestras actividades cotidianas, desde las interacciones en redes sociales hasta las transacciones en línea, generan una huella de datos significativa. La privacidad digital busca preservar la autonomía y la libertad individual al tiempo que se enfrenta a desafíos considerables relacionados con la vigilancia, la recopilación masiva de datos y la proliferación de tecnologías invasivas.

La protección de la privacidad digital no solo implica salvaguardar la información personal contra accesos no autorizados, sino también establecer límites claros sobre cómo se recopilan, utilizan y comparten los datos. En este contexto, la conciencia y la educación desempeñan un papel crucial, ya que empoderan a los individuos para tomar decisiones informadas sobre su presencia en línea y las plataformas que eligen utilizar.

F. DeepFakes

El término "deepfake" se origina de la combinación de "deep learning" (aprendizaje profundo) y "fake" (falso), y se refiere a una técnica avanzada de inteligencia artificial (IA) que emplea algoritmos de aprendizaje profundo para crear contenidos audiovisuales engañosos y extremadamente realistas. Este fenómeno ha surgido como un producto innovador de la tecnología, pero también plantea desafíos éticos significativos.

Los deepfakes utilizan modelos de inteligencia artificial entrenados con grandes conjuntos de datos de imágenes y videos para aprender patrones específicos, como expresiones faciales, gestos y tono de voz de personas reales. Posteriormente, estos modelos pueden generar contenido que simula con sorprendente precisión la apariencia y comportamiento de individuos, incluso aquellos que no participaron en la creación del contenido. Si bien los deepfakes tienen aplicaciones potenciales en campos como el entretenimiento y la producción audiovisual, su uso indebido ha generado preocupaciones considerables. La capacidad de crear vídeos o grabaciones falsas de figuras

públicas o individuos comunes conlleva riesgos significativos para la reputación y la confianza en la información visual y auditiva.

Las implicaciones éticas y legales de los deepfakes han llevado a un aumento en la conciencia sobre la necesidad de desarrollar tecnologías de detección y contramedidas. Además, varios gobiernos y plataformas en línea están trabajando para establecer regulaciones y políticas que aborden la proliferación y el mal uso de los deepfakes, buscando equilibrar la innovación tecnológica con la protección de la integridad y autenticidad de la información visual y auditiva en la era digital. Sin embargo, "en el lado humano para el correcto uso de esta tecnología se deben poner límites de respeto y privacidad, de manera que no repercuta de manera negativa en la vida de las personas humillando a una persona sin su consentimiento" (Dominguez, 2021)

Combinar datos personales implica la acción de integrar información proveniente de diversas fuentes para crear un conjunto de datos más completo y enriquecido. En el ámbito de la inteligencia artificial, esta práctica se utiliza para mejorar la calidad y la precisión de los datos, permitiendo a los algoritmos obtener una visión más detallada de los individuos. No obstante, se deben abordar cuidadosamente las consideraciones éticas y de privacidad, ya que la combinación de datos puede revelar información más sensible y plantear preocupaciones sobre la identificación individual. En el ámbito de datos personales e inteligencia artificial, la acción de combinar adquiere un significado específico. Combinar datos personales implica integrar información proveniente de diversas fuentes con el fin de crear un conjunto de datos más completo y enriquecido. Esta práctica es comúnmente utilizada para mejorar la precisión, la calidad y la utilidad de los datos en el contexto de aplicaciones de inteligencia artificial.

Al combinar datos personales, los algoritmos de inteligencia artificial pueden beneficiarse al obtener una visión más holística y detallada de los individuos, permitiendo análisis más precisos y personalizados. Sin embargo, esta acción también plantea desafíos éticos y de privacidad, ya que la combinación de datos puede revelar información más sensible o permitir la identificación directa de individuos.

La protección de datos personales se vuelve fundamental al abordar la combinación de datos en el ámbito de la inteligencia artificial. Se requiere un enfoque cuidadoso para garantizar que la recopilación y el uso de información se realicen en conformidad con las regulaciones de privacidad, respetando los derechos y la autonomía de los individuos.

G. Fusionar

Fusionar datos implica la integración completa de conjuntos de información para crear un conjunto de datos unificado y coherente. En el ámbito de la inteligencia artificial, la fusión de datos busca consolidar la información de manera que proporcione una visión global y sin fisuras. Al fusionar datos personales, se busca obtener una comprensión más completa de los perfiles individuales, pero esto también conlleva responsabilidades éticas y legales para garantizar la privacidad y el cumplimiento de las regulaciones pertinentes. La fusión de datos debe llevarse a cabo con precaución, considerando las implicaciones para la protección de la información sensible y el respeto de los derechos individuales.

En el proceso de fusión de datos personales, se busca superar las limitaciones asociadas con la fragmentación de la información, permitiendo análisis más profundos y personalizados. Sin embargo, este enfoque también plantea desafíos éticos y de privacidad, ya que la combinación completa de datos puede revelar información más detallada y sensible, aumentando el riesgo de identificación individual.

La protección de datos personales se convierte en un elemento crucial al abordar la fusión de datos en la inteligencia artificial. Se requiere un riguroso cumplimiento de las regulaciones de privacidad para garantizar que la integración de información se realice de manera ética y respetuosa con los derechos de los individuos. La transparencia en el proceso de fusión y el consentimiento informado son aspectos esenciales para salvaguardar la privacidad en este contexto, equilibrando la utilidad de la información consolidada con la necesidad de preservar la confidencialidad y autonomía de los usuarios.

H. Sustituir

La sustitución de datos se refiere al acto de reemplazar ciertos valores en un conjunto de datos con otros valores específicos. Este proceso puede ser utilizado por razones de privacidad, donde se sustituyen detalles identificables por datos ficticios o generados de manera que no se pueda asociar directamente a un individuo. Es una técnica común en el anonimato de datos para proteger la información sensible.

Sustituir datos personales implica el acto de reemplazar ciertos valores o detalles identificables en un conjunto de datos con información ficticia o generada de manera que no se pueda vincular directamente a un individuo real. Esta técnica es comúnmente utilizada en procesos de anonimato para proteger la privacidad de los datos. Sin embargo, es esencial realizar este proceso con cautela y seguir las mejores prácticas para garantizar que la sustitución no comprometa la utilidad del conjunto de datos y que se cumplan los requisitos legales y éticos relacionados con la privacidad de la información personal.

I. Simular

La simulación, en el contexto de datos, implica la creación o generación de datos que imitan el comportamiento o las características de conjuntos de datos reales. Esta técnica se utiliza en diversos campos, como la investigación y desarrollo de modelos, para probar escenarios sin utilizar datos reales. Sin embargo, la simulación también puede plantear desafíos éticos si no se utiliza con precaución y transparencia, especialmente en situaciones donde se pueda malinterpretar la autenticidad de los resultados.

Simular datos personales en el contexto de inteligencia artificial implica la creación o generación de datos ficticios que imitan las características y patrones de información personal real. Esta práctica es utilizada con fines diversos, como el desarrollo y prueba de modelos de inteligencia artificial sin comprometer la privacidad de los individuos reales. Sin embargo, se deben abordar cuestiones éticas y de transparencia para garantizar que la simulación se realice de manera ética y no genere resultados engañosos.

2. Elementos

Este análisis multidisciplinario busca abordar el vacío normativo generado por el rápido avance de la IA y su aplicación efectiva en el marco legal existente.

En su introducción, la tesis plantea el problema y justifica la relevancia de la investigación, estableciendo objetivos claros para la exploración de desafíos y perspectivas en esta confluencia. El marco teórico se sumerge en la legislación ecuatoriana, destacando la Constitución de 2008 y la Ley Orgánica de Protección de Datos Personales de 2021, delineando el contexto normativo.

La revisión de la literatura profundiza en estudios previos sobre la protección de datos y la interacción con la IA, incluyendo casos relevantes y desarrollos tecnológicos. La metodología describe el enfoque adoptado y justifica las decisiones metodológicas para la investigación.

El desarrollo constituye la parte central, explorando detalladamente la confluencia entre la protección de datos y la IA. Se analizan desafíos y vacíos normativos, centrándose en fenómenos emergentes como los deepfakes y su impacto en los derechos individuales. Las conclusiones recapitulan los hallazgos clave y reflexionan sobre las implicaciones legales y éticas, señalando áreas para investigaciones futuras.

La bibliografía incluye todas las citas y referencias bibliográficas utilizadas en la tesis, respaldando la investigación. Los anexos proporcionan documentos adicionales, como entrevistas o encuestas. El resumen ofrece una síntesis concisa de los principales puntos abordados en la tesis. En conjunto, estos elementos proporcionan una estructura completa y sistemática para la investigación.

3. Naturaleza jurídica

La naturaleza jurídica de la tesis se configura como un análisis exhaustivo que sumerge sus raíces en la intersección entre la protección de datos personales y la implementación de la Inteligencia Artificial (IA) en el marco legal de Ecuador. Este enfoque responde a la imperante necesidad de comprender y abordar las complejidades normativas que emergen en el dinámico cruce entre la salvaguarda de la privacidad y el progresivo avance de la tecnología.

En el centro de la investigación se encuentra una profunda exploración de las disposiciones legales que gobiernan la protección de datos en Ecuador, desde la Constitución de 2008 hasta la reciente Ley Orgánica de Protección de Datos Personales de 2021. El análisis se adentra en las implicaciones de estas normativas en un contexto donde la IA se posiciona como un actor significativo, generando vacíos y desafíos sustanciales en la aplicación efectiva de las leyes existentes.

El componente multidisciplinario se manifiesta en la fusión de esferas del derecho y la tecnología, donde se explora detalladamente el fenómeno de los deepfakes como manifestación de la intersección entre la manipulación digital y los derechos individuales. La tesis se erige como un documento académico que no solo revisa la literatura legal, sino que también se sumerge en los aspectos éticos y tecnológicos que caracterizan esta convergencia, estableciendo una conexión profunda entre el desarrollo normativo y las realidades prácticas en la era digital.

En última instancia, la naturaleza jurídica de la tesis se revela como un esfuerzo integrador y reflexivo que va más allá de la mera interpretación legal. Constituye un llamado a adaptar y complementar la legislación vigente para abordar específicamente las complejidades de la IA en relación con la protección de datos en Ecuador. La evolución constante de la normativa, marcada por la necesidad de preservar la privacidad en un entorno tecnológico dinámico, subraya la relevancia de este análisis multidisciplinario y su contribución a la comprensión y solución de los retos emergentes en la convergencia de la ley y la tecnología.

Como autoras, este documento representa una inmersión profunda en el entramado jurídico y tecnológico que configura el panorama de la protección de datos personales frente al avance acelerado de la Inteligencia Artificial (IA) en el contexto ecuatoriano. Desde nuestra perspectiva, este trabajo refleja un compromiso por analizar y elucidar la compleja relación entre la normativa legal existente y los desafíos emergentes generados por la IA.

La exploración de los antecedentes históricos jurídicos nos ha permitido trazar un recorrido contextual desde la promulgación de la Constitución de 2008 hasta la consolidación de la Ley Orgánica de Protección de Datos Personales

(LOPD) en 2018. Estos hitos legales sentaron las bases fundamentales que guiaron la regulación de la privacidad y la protección de datos en Ecuador.

Nuestra labor como autoras no solo radica en exponer la situación actual, sino también en proponer una perspectiva proactiva para orientar el desarrollo de políticas y regulaciones más actualizadas y coherentes. Abogamos por una revisión constante de la normativa en protección de datos para afrontar los desafíos éticos y legales que la IA plantea, garantizando así la integridad y el respeto a la privacidad en un entorno tecnológico en constante transformación.

CAPITULO II

4. El avance de la inteligencia artificial

La inteligencia artificial (IA) es un campo de la informática que se especializa en el desarrollo de agentes artificiales con autonomía de raciocinio, aprendizaje y producción. Con los avances tecnológicos, esta herramienta promete realizar actividades conectadas al "pensamiento humano", basándose en la información recolectada en su sistema para poder crear y transmitir sus propias respuestas. Esta automatización de actividades deber ser capaz de simular el comportamiento humano, imitarlo, y realizar un resultado. Martínez (2013) comprende por inteligencia artificial lo siguiente:

> Los sistemas computacionales, en la inteligencia artificial, deben ser capaces de simular características que son comúnmente asociadas con la inteligencia de la conducta humana. Un sistema inteligente es aquel que exhibe un comportamiento similar al humano cuando se enfrenta a un problema idéntico y no seamos capaces de distinguir entre un ser humano y un programa de computadora en una conversación a ciegas. (p.828)

Por lo tanto, los programas con inteligencia artificial se basan en la recopilación de información proporcionada por el usuario, con la finalidad de que este fabrique una respuesta, y al mismo tiempo adquiere mayor conocimiento con la información que va adquiriendo por parte de sus usuarios.

5. Redes Generativa Adversariales (Generative Adversial Network, o conocido por sus siglas en inglés GAN)

Las redes generativas adversariales son un tipo de modelo de inteligencia artificial que consta de un generador que crea datos, y un discriminador que evalúa la autenticidad de esos datos. Este tipo de modelo fue propuesto por Ian Goodfellow et al, en el año de 2014, y buscaba que la capacidad para generar datos nuevos sea difícil de distinguir de los datos reales, a través de su generador y discriminador, y el continuo proceso de que revisión entre ellos.

El generador se enfoca en crear contenido a base de los datos, como imágenes y sonido, que contenía en el sistema. Conforme va evolucionando en la creación de su contenido, se prepara para la generación de datos cada vez más similares a los reales. Respecto al discriminador, su rol es diferenciar los datos provenientes del sistema, y detectar qué datos fabricados por el generador y cuáles no. Goodfellow (2014) estableció lo siguiente de este tipo de sistema:

> En el marco propuesto de redes adversariales, el modelo generativo se enfrenta a un adversario: un modelo discriminativo que aprende a determinar si una muestra proviene de la distribución del modelo o de la distribución de datos. El modelo generativo puede considerarse análogo a un equipo de falsificadores, intentar producir moneda falsa y utilizarla sin ser detectado, mientras que el modelo discriminativo es de manera análoga a la policía, intenta detectar la moneda falsa. (…) Ambos equipos deben mejorar sus métodos hasta que las falsificaciones sean indistinguibles de las genuinas. (p.1)

No obstante, Goodfellow determinó que el discriminador poco a poco iba perdiendo su habilidad ante el generador que se volvía más fuerte en la elaboración de datos.

6. Sistemas informáticos deepfake

El termino deepfake fue empleado por primera vez en noviembre en el año 2017 en un foro de la plataforma de Reddit. Este término se refiere a sistemas informáticos que hacen uso de la inteligencia artificial para fabricar contenido auditivos y audiovisuales que emulan la realidad. Este contenido hiperrealista ha planteado diversas complicaciones en la sociedad, entre ellas, poder diferenciar lo que es real.

La mayoría de las deepfakes hacen uso del modelo Generative Adversarial Networks, a continuación, GAN, para la creación de su contenido. Primeramente, se requiere un conjunto de datos para poder entrenar al sistema, para que sucesivamente pueda crear el contenido deseado. Una vez que éste haya sido entrenado, es capaz de crear imágenes, videos o audios realistas, con los datos proporcionados al sistema de la persona que se quiere modificar sus datos.

Aunque este tipo de fenómenos no es nuevo, cabe resaltar que su desarrollo y elaboración requiere una menor inversión de tiempo. Los Mitra et al (2022) establece que:

> Los GAN han mejorado la calidad de las imágenes generadas [6, 10, 17, 33]. Actualmente, los enfoques GAN han logrado un éxito monumental en la creación de imágenes sintéticas [15-17, 36] y en la transferencia de estilos de imagen entre diferentes dominios [41]. La traducción de imagen a imagen puede utilizarse en el cambio de estación de una foto, la mejora de fotos, la transfiguración de objetos, etc. [41]. Pero estas aplicaciones también pueden utilizarse de forma negativa. Es difícil para la gente distinguir entre una imagen deepfake generada por GAN y una imagen real a simple vista. Estas imágenes falsas difunden desinformación a través de las redes sociales o los canales de noticias. Falsificar la identidad de alguien ("deepfake") en las redes sociales puede tener repercusiones sociopolíticas, además de riesgos financieros y de seguridad. Durante más de un siglo, los medios audiovisuales han presentado la verdad, registrando el tiempo y la historia. Pero las imágenes, vídeos y audios falsos cambian la percepción de la verdad o la realidad. Por ello es importante estudiar las amenazas que plantean las imágenes o vídeos deepfake generados por GAN. (p.3)

A pesar de las aplicaciones positivas, se señala que estas tecnologías también pueden tener usos negativos. La capacidad de los GAN para generar imágenes realistas dificulta que las personas distingan entre una imagen deepfake generada por GAN y una imagen real a simple vista.

De igual forma, se discuten los desafíos éticos y de seguridad asociados con la proliferación de imágenes deepfake. Falsificar la identidad de alguien en las redes sociales mediante deepfakes puede tener consecuencias sociopolíticas, riesgos financieros y amenazas a la seguridad. Además, se destaca que la manipulación de imágenes, videos y audios falsos puede alterar la percepción de la verdad y la realidad, lo que subraya la importancia de estudiar y comprender las amenazas que plantean las imágenes o vídeos deepfake generados por GAN.

7. La ausencia de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial.

El Código Orgánico Integral Penal tipifica el delito de delito de violación a la intimidad de la siguiente forma:

> Art. 178.-Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.
>
> No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. (p.75)

El Código Orgánico Integral Penal no prevé en el presente artículo la distribución, creación, simulación, combinación, fusión, y sustitución de contenido fabricado con los datos personales de un individuo a través de sistemas de inteligencia artificial.

El vacío en la legislación con respecto a la creación de contenido con datos personales de un individuo puede dejar a las personas en una situación de vulnerabilidad o desprotección. La ausencia de disposiciones legales específicas para abordar la distribución de contenido simulado puede dejar a las personas desprotegidas frente a nuevas amenazas tecnológicas, como deepfakes o manipulaciones digitales avanzadas.

La creación y distribución de contenido simulado, especialmente si involucra datos personales, puede resultar en un grave daño a la reputación y privacidad de las personas afectadas. Este tipo de contenido falso puede ser utilizado maliciosamente para difamar, acosar o engañar a individuos.

Ser víctima de la distribución de contenido simulado puede tener un impacto significativo en la salud mental y bienestar emocional de las personas afectadas, el impacto social de enfrentar la difusión de información falsa puede ser perjudicial. Además, las consecuencias de la distribución de contenido simulado no se limitan a lo personal, ya que pueden tener efectos sociopolíticos y económicos significativos, afectando la confianza en las instituciones, la toma de decisiones y la estabilidad de una sociedad.

La rápida evolución de la tecnología y las tácticas de manipulación digital requiere que la legislación se adapte continuamente para abordar las nuevas formas de amenazas. La falta de cobertura específica para contenido simulado puede indicar la necesidad de revisar y mejorar la legislación existente.

8. Proposición de Ley Orgánica para regular las simulaciones de imágenes y voces generadas por inteligencia artificial en España

En respuesta a esta problemática, España ha dado un paso significativo con la presentación, el 13 de octubre de 2023, de una Proposición de Ley Orgánica para regular las simulaciones de imágenes y voces generadas por inteligencia artificial. Esta iniciativa legislativa reconoce la imperante necesidad de establecer marcos legales sólidos frente a la amenaza emergente que implica esta tecnología, especialmente teniendo en cuenta que desde el año 2009 el Tribunal Europeo de Derechos Humanos ha reconocido como una dimensión ineludible del derecho a la intimidad, el control de la propia imagen.

La Proposición de Ley aboga por modificar normativas existentes. Partiendo de que la regulación de la inteligencia artificial implica reformar el ordenamiento jurídico español, esta iniciativa busca abordar las modificaciones legislativas consideradas más inmediatas y urgentes. Estas modificaciones se centran en áreas críticas, como el acceso a información veraz y la protección de derechos fundamentales, enfocándose especialmente en aspectos como la privacidad y la intimidad.

Entre las reformas, se encuentra las siguientes:

- Artículo 211. La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante. Salvo previa autorización expresa de la persona o personas afectadas, las simulaciones de imágenes, vídeos o audios de voz de estas generados a través de sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial que fueran difundidos a través de redes sociales serán consideradas como injurias hechas con publicidad.

- Artículo 727. Medidas cautelares específicas. Conforme a lo establecido en el artículo anterior, podrán acordarse, entre otras, las siguientes medidas cautelares: […] 12.ª La retirada de las simulaciones de imágenes, vídeos o voces de personas, generadas por sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial a petición de la persona afectada o sus representantes.

- Único. Se modifica el artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, añadiendo un apartado 9, quedando redactado el artículo de la siguiente forma: «Artículo 7. Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley: […] 9. La difusión y utilización de imágenes y vídeos de personas o audios de voz generados a través de sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial sin la previa autorización o consentimiento expreso de la persona o personas afectadas, excepto que incluyan de forma clara y sobresaliente una advertencia de su condición de imagen o audio de voz generado artificialmente por inteligencia artificial. La advertencia deberá figurar sobreimpresa y legible en la propia imagen. Para el caso de los audios de voz deberá realizarse una advertencia audible antes y después de su difusión.

9. Ley de Seguridad en Línea de 2023 de Reino Unido

La Ley de Seguridad en Línea de 2023 (Online Safety Act 2023) es una ley del Reino Unido que tiene como objetivo hacer que internet sea más seguro para las personas, especialmente los niños. La ley impone nuevas obligaciones a los proveedores de servicios en línea (OSP), como las redes sociales, los motores de búsqueda y las plataformas de alojamiento de contenido. Entre las principales obligaciones de la ley, se incluyen las siguientes:

- Proteger a los niños de contenido dañino, como material pornográfico, discurso de odio y acoso.
- Tomar medidas para prevenir la propagación de desinformación y noticias falsas.
- Revisar los contenidos generados por los usuarios para detectar material ilegal o dañino.
- Eliminar rápidamente el contenido ilegal o dañino cuando se les informe de ello.

Respecto al artículo relevante para nuestro trabajo, cabe mencionar que el Art. 188 de la presente ley se establece que es un delito la distribución de contenido pornográfico que simula o parece la persona en cuestión afectada, tal y como se muestra a continuación:

> 188 compartir o amenazar con compartir una fotografía o película íntima En la Ley de delitos sexuales de 2003, después del artículo 66A (insertado por el artículo 187), insertar-
>
> "66B Compartir o amenazar con compartir una fotografía o película íntima
>
> (1) Una persona (A) comete un delito si-
>
> (a) Comparte intencionadamente una fotografía o película que muestra, o parece mostrar a otra persona (B) en un estado íntimo,
>
> (b) B no consiente en que se comparta la fotografía o película, y
>
> (c) A no cree razonablemente que B consiente.
>
> (2) Una persona (A) comete un delito si-

(a) Comparte intencionadamente una fotografía o película que muestra, o parece mostrar a otra persona (B) en un estado íntimo,

(b) A lo hace con la intención de causar a B alarma, angustia o humillación, y

(c) B no consiente en que se comparta la fotografía o película.

(3) Una persona (A) comete un delito si-

(a) Comparte intencionadamente una fotografía o película que muestra o parece mostrar a otra persona (B) en un estado íntimo,

(b) A lo hace con el propósito de que A u otra persona obtenga gratificación sexual,

(c) B no consiente en que se comparta la fotografía o película, y

(d) A no cree razonablemente que B consiente.

(4) Una persona (A) comete un delito si

(a) amenaza con compartir una fotografía o película que muestre, o

parece mostrar a otra persona (B) en un estado íntimo, y

(b) lo hace

(i) con la intención de que B u otra persona que conozca a

B tema que la amenaza se lleve a cabo, o

(ii) siendo imprudente en cuanto a si B u. (p.167)

CONCLUSIONES

Concluyendo esta exhaustiva exploración multidisciplinaria, emerge la imperante necesidad de una adaptación normativa que refleje la complejidad inherente a la convergencia entre la protección de datos personales y el vertiginoso avance de la Inteligencia Artificial (IA) en Ecuador. El tejido legal, delineado por la Constitución de 2008 y la Ley Orgánica de Protección de Datos Personales de 2021, aunque crucial, revela ciertos vacíos cuando se enfrenta a los desafíos surgidos con la irrupción de la IA.

En primer lugar, es evidente que la legislación actual, concebida en un periodo previo al auge significativo de la IA, requiere de ajustes y complementos específicos para abordar las complejidades éticas y jurídicas inherentes a esta tecnología. La evolución constante de la IA plantea desafíos que van más allá de los marcos normativos tradicionales, demandando una revisión proactiva que incorpore principios éticos, responsabilidad algorítmica y garantías específicas para proteger los derechos individuales.

En segundo lugar, el fenómeno de los deepfakes, analizado detalladamente en este trabajo, representa un claro ejemplo de las lagunas normativas actuales. La ausencia de regulaciones específicas que aborden la creación, distribución y manipulación de contenidos generados por IA refleja una brecha que permite el uso indebido de esta tecnología para violar derechos fundamentales como la privacidad, el honor y la propia imagen. En este sentido, urge la implementación de disposiciones legales que establezcan límites y sanciones claras frente a la manipulación digital de la realidad.

En conclusión, el presente análisis subraya la necesidad inminente de una revisión integral de la normativa ecuatoriana en protección de datos, considerando la dinámica evolución de la IA. La adaptación de la legislación no solo debe abordar la convergencia de la protección de datos y la IA, sino también anticiparse a las posibles ramificaciones éticas y jurídicas que las tecnologías emergentes podrían introducir en el futuro. Este llamado a la acción representa una invitación a los legisladores y tomadores de decisiones a promover una legislación actualizada, ética y eficiente que preserve los derechos fundamentales en el paisaje cambiante de la tecnología y el derecho en Ecuador.

RECOMENDACIONES

Se propone las siguientes recomendaciones:

- Que se agregué el siguiente artículo innumerado en la Sección Sexta, que versa sobre los Delitos contra el derecho a la intimidad personal y familiar, después del Art. 178 del Código Orgánico Integral Penal:

  Art. (…) – Utilización indebida de sistemas de inteligencia artificial y tecnologías relacionadas. - La persona que, sin contar con el consentimiento o la autorización legal, cree, genere, manipule y divulgue contenido falso utilizando tecnologías de aprendizaje profundo, con el propósito de engañar, manipular o causar daño a terceros, será sancionada con pena privativa de libertad de uno a tres años.

- Que el Art. 178 del Código Orgánico Integral Penal se agregue el siguiente párrafo después del primer párrafo del artículo:

  "También se considera como violación a la intimidad el uso sistemas de inteligencia artificial con el fin de recopilar, procesar, generar, manipular, o difundir información personal, mensajes electrónicos, voz, audio, video, o cualquier otro tipo de dato protegido por la legislación ecuatoriana."

  El artículo reformado quedaría de la siguiente forma:

  Art. 178.-Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

  También se considera como violación a la intimidad el uso sistemas de aprendizaje profundo con el fin de recopilar, procesar, generar, manipular, o

difundir información personal, mensajes electrónicos, voz, audio, video, o cualquier otro tipo de dato protegido por la legislación ecuatoriana.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

- Adaptación Normativa Continua

En concreto a nuestro basto estudio, análisis, e interpretación de la normativa jurídica, ya que es imperativo abogar por una adaptación legal continua en la que se refleje la rápida evolución de la Inteligencia Artificial (IA), recomendamos la revisión regular de la legislación en protección de datos para incorporar disposiciones específicas que aborden los desafíos y riesgos emergentes asociados con el uso de la IA, asegurando.

BIBILOGRAFÍA

Abbott, R. (2020) The Reasonable Robot: Artificial Intelligence and the Law by Professor. Submitted for the Degree of Doctor of Philosophy. School of Law Faculty of Arts and Social Sciences University of Surrey

Caldwell, M., Andrews, J.T.A., Tanay, T. *et al.* AI-enabled future crime. *Crime Sci* **9**, 14 (2020). https://doi.org/10.1186/s40163-020-00123-8

Comisión Europea (2021). Propuesta De Reglamento Del Parlamento Europeo Y Del Consejo Por El Que Se Establecen Normas Armonizadas En Materia De Inteligencia Artificial (Ley De Inteligencia Artificial) Y Se Modifican Determinados Actos Legislativos De La Unión. Recuperado De Https://Eur-Lex.Europa.Eu/Resource.Html?Uri=Cellar:E0649735-A372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&Format=PDF

Constitución de la República del Ecuador. (25 de enero de 2021). Registro Oficial 449. Recuperado el 28 de febrero de 2024, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Daus, G. (27 de septiembre de 2019). *Deepfakes: chantajes y mentiras en el videoclub. Entrevista a Sam Gregory, experto y activista de DDHH internacional.* Recuperado el 17 de febrero de 2024, de https://www.clarin.com/revista-enie/ideas/deepfakes-chantajes-mentiras-videoclub_0_x4sN0a52.html

Domínguez, A. (25 de mayo 2021). ¿Qué es la tecnología deepfake? Usos, ventajas y desventajas. Recuperado el 25 de febrero de 2024, de https://marketinginsiderreview.com/tecnologia-deepfake-que-es-publicidad/

Gobierno de España (19 de abril de 2023). *Plan de Recuperación, Transformación y Resiliencia.* Recuperado el 16 de febrero del 2024, de https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr#:~:text=La%20inteligencia%20artificial%20(IA)%20es,el%20razonamiento%20y%20la%20percepci%C3%B3n.

Ley Orgánica de Protección de Datos. (26 de mayo 2021). Registro Oficial Suplemento 459. Recuperado el 28 de febrero de 2024, de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Mestre, E. (9 de diciembre de 2023). *Bases de datos Jurídicas: Qué son y tipologías. 1.ª parte. Recuperado el 14 de marzo de 2024, de* https://www.ticdoc.net/es/2020/12/09/bases-de-datos-juridicas-que-son-y-tipologias-1-a-parte/

Quinto Suplemento del Registro Oficial No.459, 26 de mayo 2021. Ley Orgánica De Protección de Datos Personales.

Rogers, J., & Bell, F. (2019). The Ethical AI Lawyer: What is Required of Lawyers When They Use Automated Systems?. Law, Technology and Humans, 1, 80-99. https://doi.org/10.5204/lthj.v1i0.1324

Santos, J. (6 de febrero de 2024). ¿Qué es la privacidad digital y cómo mejorarla en tu empresa? Recuperado el 9 de marzo de 2024, de https://www.deltaprotect.com/blog/privacidad-digital#:~:text=La%20privacidad%20digital%20o%20privacidad,personas%20o%20instituciones%20a%20estos.

Tercer Suplemento del Registro Oficial No.435, 13 de noviembre 2023. Decreto No. 904 (Reglamento General de la Ley Orgánica De Protección de Datos Personales).

University College London. (4 de agosto de 2020). Deepfakes clasificada como la amenaza de crimen de IA más grave", artículo en web. Universidad College, Londres. Recuperado de https:// www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

Wong, A. (2021). Ethics and Regulation of Artificial Intelligence.

DECLARACIÓN Y AUTORIZACIÓN

Nosotras, **Morales Tambo, Jessica Anabel** con C.C: # 0932462518; y **Parrales Aveiga, Andrea Michelle** con C.C: # 0926926627, autoras del trabajo de titulación: **Impacto de la Inteligencia Artificial en la Privacidad y Seguridad en la Era Digital,** previo a la obtención del título de ABOGADA en la Universidad Católica de Santiago de Guayaquil.

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

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

Guayaquil, **23** de **abril** de **2024**

f. _____

Morales Tambo, Jessica Anabel

C.C: # 0932462518

f. _____

Parrales Aveiga, Andrea Michelle

C.C: # 0926926627

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Impacto de la Inteligencia Artificial en la Privacidad y Seguridad en la Era Digital		
AUTOR(ES)	Morales Tambo, Jessica Anabel Parrales Aveiga, Andrea Michelle		
REVISOR(ES)/TUTOR(ES)	Abg. García Auz, Jose Miguel, Mgs.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia y Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TITULO OBTENIDO:	Abogada		
FECHA DE PUBLICACIÓN:	**23** de **abril** de **2024**	**No. DE PÁGINAS:**	26
ÁREAS TEMÁTICAS:	Derecho Penal, Derecho Internacional y Derecho Constitucional		
PALABRAS CLAVES/ KEYWORDS:	Sistemas de Inteligencia Artificial (IA), Base de datos, Protección de datos personales, Consentimiento, Privacidad Digital, DeepFakes, Combinar, Fusionar, Sustituir, Simular		

RESUMEN/ABSTRACT (150-250 palabras):

En el escenario jurídico de Ecuador, la intersección entre la protección de datos y la cada vez más extendida implementación de sistemas de Inteligencia Artificial (IA) presenta una red de desafíos que se entrelazan en una compleja ambigüedad normativa. Esta investigación, respaldada por un enfoque interdisciplinario que amalgama análisis jurídicos y tecnológicos, se sumerge en esta intrincada maraña para no solo comprender, sino también resolver, la incertidumbre que surge al aplicar las regulaciones de protección de datos a la IA. El examen exhaustivo aborda la esencia misma, los orígenes y las ramificaciones de esta ambigüedad, con un énfasis particular en los desafíos asociados a la asignación de responsabilidades y a la preservación de la privacidad. El presente estudio no se limita a una mera exploración superficial; por el contrario, se adentra en una investigación minuciosa y detallada, con el foco puesto en identificar y abordar los desafíos complejos que emergen en este cruce entre el ámbito jurídico y tecnológico. Su propósito es ofrecer soluciones concretas y efectivas que puedan moldear el panorama normativo del país, específicamente en la era desafiante y fascinante de la Inteligencia Artificial.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-4-**(registrar teléfonos)**	E-mail: jessicamoralestambo@gmail.com andrea.parrales07@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: Reynoso Gaute, Maritza Ginette**	
	Teléfono: +593-4-3804600	
	E-mail: maritza.reynoso@cu.ucsg.edu.ec	

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