



1859

UNL

Universidad
Nacional
de Loja

Universidad Nacional de Loja
Facultad Jurídica Social Administrativa
Carrera de Derecho

“La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”

**Trabajo de Integración
Curricular previo a la obtención
del Título de Abogada.**

AUTORA:

Evelyn del Carmen Vargas Granda

DIRECTOR:

Dr. Guilber René Hurtado Herrera, Mg. Sc.

Loja - Ecuador

2024

Certificación



unl

Universidad
Nacional
de Loja

Sistema de Información Académico
Administrativo y Financiero - SIAAF

CERTIFICADO DE CULMINACIÓN Y APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo, **HURTADO HERRERA GUILBER RENE**, director del Trabajo de Integración Curricular denominado **LA MANIPULACIÓN DE ARCHIVOS DE VIDEO, IMAGEN O VOZ UTILIZANDO LA INTELIGENCIA ARTIFICIAL VULNERA EL DERECHO A LA INTIMIDAD PERSONAL Y FAMILIAR**", perteneciente al estudiante **EVELYN DEL CARMEN VARGAS GRANDA**, con cédula de identidad N° **1150648739**.

Certifico:

Que luego de haber dirigido el **Trabajo de Integración Curricular**, habiendo realizado una revisión exhaustiva para prevenir y eliminar cualquier forma de plagio, garantizando la debida honestidad académica, se encuentra concluido, aprobado y está en condiciones para ser presentado ante las instancias correspondientes.

Es lo que puedo certificar en honor a la verdad, a fin de que, de así considerarlo pertinente, el/la señor/a docente de la asignatura de **Integración Curricular**, proceda al registro del mismo en el Sistema de Gestión Académico como parte de los requisitos de acreditación de la Unidad de Integración Curricular del mencionado estudiante.

Loja, 2 de Agosto de 2024



Resuelto y autorizado por:
GUILBER RENE
HURTADO HERRERA

F) -----
DIRECTOR DE TRABAJO DE INTEGRACIÓN
CURRICULAR



Certificado TIC/TT.: UNL-2024-001823

1/1
Educamos para **Transformar**

Autoría

Yo, **Evelyn del Carmen Vargas Granda**, declaro ser autora del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente, acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Integración Curricular, en el Repositorio Digital Institucional - Biblioteca Virtual.

Autora: Evelyn del Carmen Vargas Granda

Cédula: 1150648739

Fecha: 11 de diciembre de 2024

Correo electrónico: evelyn.vargas@unl.edu.ec

Teléfono: 0985695277

Carta de autorización

Carta de autorización por parte de la autora, para consulta, reproducción parcial o total y/o publicación electrónica del texto completo del Trabajo de Integración Curricular.

Yo, **Evelyn del Carmen Vargas Granda** declaro ser la autora del Trabajo de Integración Curricular denominado: **“La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”**, como requisito para optar el Título de Abogada, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja, para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 11 días de Diciembre de 2024.

Autora: Evelyn del Carmen Vargas Granda

Cédula: 1150648739

Fecha: 11 de diciembre de 2024

Correo electrónico: evelyn.vargas@unl.edu.ec

Teléfono: 0985695277

DATOS COMPLEMENTARIOS.

Director de Trabajo de Integración Curricular: Dr. Guilber René Hurtado Herrera Mg. Sc.

Dedicatoria

Dedico esta tesis a mi padre, que sin su apoyo incondicional no hubiera podido alcanzar este logro tan importante; a mi ángel, mi madre, quien a pesar de no estar físicamente presente, su fortaleza y amor incondicional siguen siendo el pilar que me sostiene día a día; a mi Camila y Meyli, que a través de su amor genuino e inocente han sido mi fortaleza en muchos momentos de mi vida; y, a mi Gabriel Alejandro, mi compañero incondicional, que siempre está a mi lado para brindarme su apoyo y amor sincero.

Evelyn del Carmen Vargas Granda.

Agradecimiento.

Expreso mi más profundo agradecimiento a la Universidad Nacional de Loja, que me brindó la oportunidad de formarme en sus aulas durante mi carrera de Derecho. También deseo extender mi gratitud a los docentes que me han orientado en la elaboración de este trabajo, principalmente al Director de mi Trabajo de Integración Curricular, el Doctor Guilber Hurtado, quien, con su sabiduría, ética, dedicación y profesionalismo, me asesoró y aportó sus conocimientos para la correcta realización de la presente investigación.

Evelyn del Carmen Vargas Granda.

Índice de contenidos

Certificación	ii
Autoría	iii
Carta de autorización	iv
Dedicatoria	v
Agradecimiento.	vi
Índice de contenidos	vii
Índice de tablas	x
Índice de figuras	x
Índice de anexos	x
1. Título	1
2. Resumen	2
2.1. Abstract	3
3. Introducción	4
4. Marco teórico	6
4.1. Derecho informático.....	6
4.1.1. <i>Seguridad informática</i>	8
4.2. Inteligencia Artificial	10
4.2.1. <i>Beneficios de la Inteligencia Artificial</i>	11
4.2.2. <i>Riesgos de la Inteligencia Artificial</i>	14
4.2.3. <i>Regulación de la Inteligencia Artificial</i>	15
4.3. Terminología Informática.....	16
4.3.1. <i>Deepfakes</i>	16
4.3.2. <i>Machine Learning</i>	18
4.3.3. <i>Deep Learning</i>	19
4.3.4. <i>Algoritmo</i>	20

4.3.5. <i>Deepfaces y Deepvoices.</i>	21
4.3.6. <i>Ciberespacio.</i>	21
4.4. Entorno Digital	22
4.4.1. <i>Redes sociales</i>	22
4.4.2. <i>Medios cibernéticos.</i>	23
4.4.3. <i>Ciberdelitos</i>	23
4.5. Manipulación digital de archivos de video, imagen o voz	24
4.5.1. <i>Origen de la manipulación digital de archivos de video, imagen o voz</i>	24
4.5.2. <i>Herramientas utilizadas en la manipulación digital de archivos de video, imagen o voz.</i>	25
4.6. Derecho a la Intimidad Personal y Familiar	29
4.7. El Delito	33
4.7.1. <i>Estructura del delito</i>	34
5. Metodología	40
5.1. Materiales Utilizados.....	40
5.2. Métodos	40
5.3. Técnicas.....	41
6. Resultados.	41
6.1. Resultados de Encuestas.....	41
6.2. Resultados de las entrevistas	51
6.3. Estudio de casos	60
6.3.1. <i>Caso Nro. 1.</i>	61
6.3.2. <i>Caso Nro. 2</i>	62
6.3.3. <i>Caso Nro. 3.</i>	63
7. Discusión	65
7.1. Verificación de objetivos	65
7.1.1. <i>Objetivo general</i>	65
7.1.2. <i>Objetivos específicos</i>	66

7.2. Hipótesis.....	69
7.3. Fundamentación jurídica para la propuesta de Reforma Legal.....	70
8. Conclusiones	72
9. Recomendaciones	73
9.1. Propuesta de Reforma al Código Orgánico Integral Penal	75
10. Bibliografía	78
11. Anexos	84

Índice de tablas

Tabla Nro. 1.	42
Tabla Nro. 2.	44
Tabla Nro. 3.	46
Tabla Nro. 4.	48
Tabla Nro. 5.	49

Índice de figuras

Figura Nro. 1.	42
Figura Nro. 2.	44
Figura Nro. 3.	46
Figura Nro. 4.	48
Figura Nro. 5.	50

Índice de anexos

Anexo Nro. 1. Memorando de designación del Director del Trabajo de Integración Curricular o Titulación	84
Anexo Nro. 2. Formato de Encuesta	86
Anexo Nro. 3. Formato de entrevistas	89
Anexo Nro. 4. Certificación del Abstract.	92
Anexo Nro. 5. Aptitud legal	93

1. Título

“La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”

2. Resumen

El presente Trabajo de Integración Curricular titulado “La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar” aborda cómo el uso de las nuevas tecnologías genera un impacto significativo al derecho a la intimidad personal y familiar. El enfoque del presente trabajo investigativo se basa en los objetivos que incluyen, el estudio doctrinario y jurídico de cómo estas tecnologías afectan la intimidad personal y familiar, y una vez demostradas las afectaciones, presentar un proyecto de reforma legal en Ecuador para tipificar y sancionar este problema.

En este Trabajo de Integración Curricular se emplearon diversos materiales y métodos que facilitaron su desarrollo. Se llevaron a cabo encuestas y entrevistas con profesionales del Derecho y especialistas en informática. Así también, se incorporó el uso de métodos, inductivo, deductivo, hermenéutico y comparativo para asegurar un desarrollo integral de la investigación. Los resultados indican que esta situación vulnera principalmente el derecho a la intimidad personal y familiar, y destacan la imperiosa necesidad de reformar el Código Orgánico Integral Penal para proteger a los ciudadanos de estos riesgos inminentes.

Además, es sustancial resaltar la importancia de implementar campañas de concientización para educar a la sociedad sobre los peligros asociados con la manipulación digital. Este trabajo investigativo subraya la urgencia de tomar medidas legales para enfrentar los desafíos que presentan las tecnologías de la información y la comunicación, porque el derecho debe evolucionar al mismo ritmo que la tecnología y evitar vacíos legales que perjudiquen a la sociedad en general.

Palabras clave: derecho informático, manipulación, inteligencia artificial, derecho a la intimidad, reforma legal.

2.1. Abstract

This Curricular Integration research entitled “The manipulation of video, image or voice files using Artificial Intelligence violates the right to personal and family privacy” addresses how the use of new technologies generates a significant impact on the right to personal and family privacy. The objectives include the doctrinal and legal study of how these technologies affect personal and family privacy. Once the affectations are demonstrated, a project of legal reform to typify and punish this problem in Ecuador will be presented.

In this Curricular Integration research, some materials and methods were used to facilitate the development of this work. Surveys and interviews were conducted to legal professionals, computer specialists, and experts on the problem. Also, the use of inductive, deductive, hermeneutic, and comparative methods was incorporated to ensure an integral development of the research. The results indicate that this situation mainly violates the right to personal and family privacy, highlighting the urgent necessity to reform the Organic Integral Penal Code to protect citizens from these imminent risks.

In addition, it is important to highlight the importance of implementing awareness campaigns to educate society about the dangers associated with digital manipulation. This research work underlines the urgency of taking legal measures to face the challenges presented by information and communication technologies. It is because the law must evolve at the same pace as technology and avoid legal loopholes that harm society in general.

Keywords: computer law, manipulation, artificial intelligence, right to privacy, legal reform.

3. Introducción

Este trabajo de investigación consistió en un análisis detallado sobre el tema: “La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”. El presente tema genera progresiva preocupación debido a su capacidad para afectar gravemente el derecho a la intimidad personal y familiar, básicamente se trata de la generación de contenido multimedia falso con un alto grado de realismo, haciendo difícil distinguir entre lo real y lo manipulado. La presente investigación se centra en analizar este problema desde un estudio doctrinario y jurídico, se abordó lo referente al derecho informático, y en base al tema expuesto, se elaboró una minuciosa investigación sobre lo que conlleva la Inteligencia Artificial, definiendo términos, indagando el proceso y las herramientas utilizadas para la creación del contenido falso, además, se destacó aquellos sitios en donde existe la masiva difusión de estos archivos, siendo el objeto de estudio las implicaciones legales y sociales en el contexto ecuatoriano, pero también en el ámbito internacional, ya que se trata de un problema que está en auge a nivel global.

La importancia del tema radica en el potencial de esta nueva tecnología, para vulnerar los derechos de las personas. El problema planteado se enfoca en la falta de regulación adecuada, misma que permite que estas herramientas sean utilizadas con fines poco éticos, afectando derechos fundamentales, principalmente la intimidad personal y familiar. Los beneficios de abordar este tema son diversos y significativos, en primer lugar, se contribuye a la protección de los derechos individuales, garantizando que las personas mantengan su entorno digital libre de injerencias que perjudiquen su intimidad, tanto en el ámbito personal como familiar. Además, se promueve la reforma de las normativas legales existentes, adaptando el Derecho a los avances tecnológicos constantes, con el fin de evitar vacíos legales. Finalmente, se incentiva un uso ético de la tecnología, fomentando la educación en esta área e incentivando prácticas responsables, y que la sociedad ecuatoriana aproveche de la mejor manera los grandes beneficios que ofrece la tecnología en diversas áreas.

En relación con otros trabajos, esta investigación se basa en estudios previos sobre este tema, integrando conocimientos de diversas áreas para proporcionar un análisis comprensivo. Por ejemplo, el Ministerio de Telecomunicaciones y de la Sociedad de la Información realizó un proyecto de diagnóstico que comprende el tema de la Inteligencia Artificial en nuestro país, y determina lo siguiente:

La Inteligencia Artificial es un ámbito con mucho potencial en nuestro país, que, direccionada y aplicada de una manera adecuada, a través de políticas públicas acordes a estándares internacionales en concordancia con los intereses y necesidades de los diferentes actores del ecosistema digital, puede representar un habilitador trascendente en la búsqueda de lograr la transformación digital del país. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, pág. 6)

Por ende, debemos reconocer que, en Ecuador, la Inteligencia Artificial ya está en uso y en proceso de mejora para un futuro de transformación digital. Sin embargo, el análisis de la presente investigación comprende justamente la ausencia de su regulación, para con ello poder garantizar el uso ético de esta tecnología. Para lograr una transformación digital efectiva, es fundamental definir claramente qué implica esta transformación, comprender su alcance y reconocer los posibles daños que podría causar un uso indebido y malintencionado de la Inteligencia Artificial.

En virtud de ser un problema relativamente actual, en el contexto ecuatoriano existe desconocimiento por parte de la ciudadanía y un claro desinterés gubernamental sobre este tema, no se le está dando la atención que realmente amerita. En nuestro país, no existe un marco legal claro sobre este tema, en el Código Orgánico Integral Penal no se encuentra estipulado el término "manipular" mucho menos una definición precisa de "Inteligencia Artificial", lo que justificó la realización de la presente investigación.

En el presente trabajo investigativo se verifica un objetivo general que consiste en: “Realizar un estudio, doctrinario y jurídico sobre la manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial y su vulneración al derecho a la intimidad personal y familiar”. Además, se verificó los objetivos específicos que se detallan a continuación: primer objetivo específico “Establecer las afectaciones al derecho a la intimidad personal y familiar por la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial”; segundo objetivo específico: “Demostrar la vulneración a la intimidad personal y familiar por la manipulación de archivos de video, imagen o voz mediante el uso de la inteligencia artificial”; tercer objetivo específico: “Presentar un proyecto de reforma legal al régimen penal ecuatoriano, tipificando y sancionando la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial para garantizar el derecho a la intimidad personal y familiar”. La hipótesis contrastada es la siguiente: La falta de tipificación

y sanción de la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar.

El alcance de este trabajo incluyó un análisis jurídico y doctrinal, complementado con un estudio empírico basado en encuestas y entrevistas. Las limitaciones fueron la disponibilidad de datos sobre procesos judiciales acerca de este problema, por ser un vacío legal, superando las capacidades de las leyes actuales y dejando en evidencia la falta de seguridad jurídica en nuestro país. La presente investigación buscó resaltar la importancia de analizar el impacto de la Inteligencia Artificial y los riesgos que conlleva su falta de regulación, proponiendo desarrollar leyes que establezcan un marco legal claro y objetivo para garantizar el efectivo goce del derecho a la intimidad personal y familiar.

4. Marco teórico

4.1. Derecho informático

El vocablo Derecho “tiene raíz latina que deriva de la voz *directum*, que significa lo que está conforme a la regla, a la ley o la norma”. (Biblioteca del Congreso Nacional de Chile, 2024, pág. 1) Se entiende que está asociado con la rectitud, con lo justo y lo legal. Siendo así que se encarga de regular la conducta de los individuos para una correcta convivencia social. Por su parte, el término informática es definido por la RAE como el “conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores” (Real Academia Española, 2001, pág. 1) La informática se cataloga como aquella técnica que ayuda a manejar y procesar datos de forma automática en el ámbito digital, además es un aspecto fundamental para poder comprender de manera profunda todo lo referente a la gestión de la información.

Al combinar ambos aspectos, surge el Derecho Informático como aquella rama del Derecho, encargada de regular las actividades producidas en el entorno digital siendo su existencia esencial en la era de la información, y su contribución de legalidad es determinante para la protección de los derechos en este ámbito.

El Derecho Informático busca proporcionar un marco legal ante situaciones que se suscitan en el entorno digital. El Doctor Julio Téllez Valdés afirma que: “Es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.” (Téllez Valdés, 2009, pág. 13) Actualmente ya existe un ordenamiento jurídico que aborda el ámbito informático. Sin

embargo, el derecho informático no solo pretende regular el uso de la tecnología en el contexto legal, sino también comprender en profundidad los aspectos legales y éticos que surgen en torno a la informática. Asimismo, busca evolucionar continuamente para abordar nuevas formas de delitos informáticos.

Es importante destacar que el derecho informático se presenta como una especialidad que “abarca todos los marcos jurídicos relacionados con la transferencia, uso y almacenamiento de información en formato electrónico.” (Sierra , 2023, pág. 1). Esta rama jurídica establece la directa relación entre la ley y la informática. Su objetivo principal es la regulación de aquellos delitos de origen digital, y como consecuencia observamos que el derecho informático ha ido progresando constantemente para así implementar la debida protección de los derechos que se vulneran a través de medios electrónicos.

Ahora bien, hoy en día se habla de una revolución digital, de forma que el crecimiento de las redes de información es demasiado amplio y como menciona el Dr. Julio Téllez Valdés: “La revolución digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de ideas y conocimientos en todo el planeta” (Téllez Valdés, 2009, pág. 1) Según ello, la sociedad se desarrolla cada vez más con todo tipo de tecnología existente, siendo así que las TIC desarrollan un papel fundamental en nuestro día a día, desencadenando que los usuarios experimenten un constante intercambio de información derivados de suministros, programas, y personas.

La Constitución de la República del Ecuador determina lo siguiente:

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:
2. El acceso universal a las tecnologías de información y comunicación. (Constitución de la República del Ecuador, 2008, pág. 12)

Es fundamental resaltar la relevancia de este precepto constitucional, ya que garantiza el acceso libre a las tecnologías de la información y comunicación (TIC) como un derecho. La sociedad avanza hacia una mayor dependencia de estas tecnologías, sin embargo, junto con sus beneficios, es igualmente fundamental reconocer que la tecnología conlleva una serie de riesgos, por ejemplo, en internet circula una vasta cantidad de información procedente de diversas fuentes, sin que ello garantice la confiabilidad de las mismas o la veracidad del contenido compartido, además, la facilidad con la que se puede difundir contenido,

independientemente de su exactitud, permite que cualquier persona propague información que puede contribuir a la desinformación y a la expansión de datos falsos.

Por su parte, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos señala que:

Art. 1.- Objeto de la ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002, pág. 1)

Como se puede evidenciar, en nuestro país ya existe un ordenamiento jurídico sobre el Derecho Informático, el cual se encarga de regular todos los aspectos relacionados a las Tecnologías de la Información y las Comunicaciones denominadas TIC. Estas tecnologías han sido un factor importante para la innovación no solo en el Derecho si no también en una variedad de campos, por ejemplo: La educación, salud, comercio, seguridad, etc.

Teniendo en cuenta lo antes mencionado, se puede determinar que el Derecho Informático es aquella relación entre la informática y el derecho que se resume en aquel conjunto de normas que regula todo lo relacionado a las actividades realizadas por medios digitales. A medida que nuestra sociedad avanza, podemos observar que nos adentramos en un entorno cada vez más digitalizado, y el derecho es una de las ciencias que se ha visto inmersa en este avance tecnológico constante, es por esta razón que se desarrolla el derecho informático, como consecuencia de aquella necesidad de abarcar todo lo relacionado a la informática y su vinculación con el ámbito legal.

4.1.1. Seguridad informática

El Dr. Emilio Suñe, Catedrático de Filosofía Jurídica y Derecho Informático de la Universidad Complutense de Madrid, afirma que:

El Derecho de la informática, por seguir aportando razones singulares que avalan su autonomía, tiene mucho de Derecho Global, al tratarse de un Derecho muy internacionalizado, probablemente por el tipo de comunidades humanas que están en su base. La regulación jurídica de Internet, por ejemplo, plantea problemas globales, que requieren soluciones globales. Las grandes multinacionales del sector teleinformático,

que lo dominan casi todo por completo, no pueden ni quieren adaptarse a regulaciones estatales injustificadamente diversas y dispersas, cuando el mercado no es nacional, sino global (Suñe, 2017, pág. 7)

Es así que esta rama jurídica se caracteriza principalmente por su capacidad de abordar y resolver de la mejor forma cuestiones de carácter global debido a su gran trascendencia en todo el mundo. Un claro ejemplo de este ámbito es la seguridad informática, puesto que, la tecnología es un factor importante que requiere la ejecución de un marco regulatorio, para así poder operar de forma correcta en nuestra sociedad. En un entorno globalizado, el autor indica que la existencia de normativas distintas entre diferentes países puede generar conflictos innecesarios, por lo que la tendencia es hacia una homogeneización de las regulaciones para facilitar la innovación a nivel mundial.

El Ing. Gabriel Baca Urbina nos dice que:

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. (Urbina, 2017, pág. 12)

En este aspecto el autor subraya la relevancia de la seguridad informática en la protección de la información. Mediante directrices y regulaciones, busca salvaguardar la integridad y confidencialidad de la información almacenada en los sistemas digitales. Al abordar y mitigar riesgos, esta disciplina asegura que la información esté protegida de diversas amenazas, garantizando así su confiabilidad y seguridad dentro del almacenamiento de datos informáticos.

El experto en seguridad informática Alfonso García Cervigón define a la seguridad informática como: “un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático” (Cervigón, 2011, pág. 1) y esto es lo que realmente caracteriza a la seguridad informática en su aspecto general, proteger a la información que contienen aquellos sistemas informáticos es fundamental para garantizar la debida confidencialidad y prevenir accesos no autorizados, no solamente por la protección de datos si no para prevenir amenazas y ataques cibernéticos que hoy en día son más complejos y avanzados.

4.2. Inteligencia Artificial

La Inteligencia Artificial representa un campo de estudio de gran interés y relevancia en la actualidad, es admirable cómo las máquinas pueden imitar y, en muchos casos, superar las capacidades humanas en tareas cognitivas complejas. Como parte de esta investigación, considero importante comprender desde el surgimiento del término Inteligencia Artificial, hasta su relación con el ámbito legal, para así evidenciar las posibles consecuencias derivadas de su mal utilización.

Para el análisis de este tema es fundamental comenzar por definir qué es la Inteligencia Artificial. Al respecto, recurro a las palabras del reconocido experto internacional en este campo, Lasse Rouhiainen, quien define que: “la IA es la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano.” (Rouhiainen, 2018, pág. 17) El autor enfatiza que la Inteligencia Artificial tiene la capacidad de llevar a cabo diversas acciones de manera automática, como reproducir música, redactar textos, enviar mensajes, realizar llamadas de voz, traducir palabras, realizar operaciones matemáticas, ofrecer instrucciones de ubicación, entre un sinnúmero de funciones. Esta habilidad para imitar capacidades humanas es fundamental para comprender el funcionamiento de esta herramienta informática.

Para entender a fondo la Inteligencia Artificial, es importante explorar sus orígenes y cómo evolucionó a medida que la sociedad ha avanzado.

El profesor Luis Barrera Arrestegui expone:

En 1956 durante el mes de julio, se llevó a cabo la Conferencia de Verano en el Dartmouth Collage, organizada por John McCarthy a la cual asistieron otros nueve noveles científicos: Marvin Minsky, Nathaniel Rochester, Claude Shannon, Trenchard More, Arthur Samuel, Ray Solomomoff, Oliver Selfridge, Alan Newell y Herbert Simon, para presentar sus respectivos trabajos y establecer una serie de premisas de investigación para los próximos años. Esto constituyó la partida de nacimiento de la Inteligencia Artificial como campo de investigación. (Barrera, 2012, pág. 90)

El autor nos relata sobre la Conferencia de Verano en el Dartmouth College (Hanover, EEUU) en 1956, donde prácticamente se establecieron los cimientos para el desarrollo de la Inteligencia Artificial y el alcance que tendría en el futuro, marcando el comienzo de muchas

investigaciones. Desde entonces, la denominación de Inteligencia Artificial ha ganado popularidad y, con el tiempo, ha evolucionado fuertemente.

De hecho “Fue John McCarthy quien acuñó originalmente el término IA en el Dartmouth Summer Research, proyecto sobre Inteligencia Artificial. Por ello se le considera el padre de la inteligencia artificial.” (Yuchen Jiang, 2022, pág. 3) El ser humano ha utilizado y obtenido los medios necesarios para ir hacia un avance tecnológico continuo, y la Inteligencia Artificial es muestra de ello, sin embargo, la búsqueda de innovación nos lleva a la creación de sistemas cada vez más avanzados y su debida regulación se puede ver limitada.

La Inteligencia Artificial, a pesar de sus avances revolucionarios, plantea una serie de desafíos que incluyen preocupaciones éticas sobre el uso de datos personales, y afectaciones a derechos fundamentales como lo es el derecho a la intimidad personal y familiar, afectando así a la sociedad en general. Más adelante examinaremos por qué es necesario regular la Inteligencia Artificial, e indagaremos su potencial impacto en diversos aspectos de nuestra vida y la necesidad de garantizar su uso responsable.

4.2.1. Beneficios de la Inteligencia Artificial

El progreso acelerado de la Inteligencia Artificial ha abierto puertas a nivel global en diversas áreas. Ha revolucionado el marketing, ha brindado apoyo al sistema educativo, la salud, el sistema judicial y muchos otros ámbitos. Estos avances no solo optimizan procesos y servicios, sino que también abren nuevas posibilidades para el desarrollo y la innovación.

Según la Oficina de las Naciones Unidas contra la Droga y el Delito en México, actualmente se usa la Inteligencia Artificial para ayudar con la detección y prevención de violencia contra la mujer, haciendo uso de estas tecnologías se ofrece una alternativa innovadora para analizar reportes de llamadas de emergencia, en la noticia se establece que: “El Centro de Excelencia UNODC-INEGI (CdE) utiliza la Inteligencia Artificial (IA) para analizar reportes de llamadas al 911 y así detectar este tipo de violencia.” (Naciones Unidas : Oficina de las Naciones Unidas Contra la Droga y el Delito En México, 2023, pág. 1) Aquí se puede evidenciar el uso de la Inteligencia Artificial en una cuestión de suma importancia, dentro de la justicia y que se maneja de forma beneficiosa para la sociedad.

De igual forma, dentro del reporte, se determina el procedimiento usado:

El CdE desarrolló una metodología para analizar la transcripción de las llamadas y detectar aquellas que fueron clasificadas bajo un tipo de violencia distinto, pero donde puede detectarse un caso de violencia contra la mujer a partir del uso de redes neuronales artificiales para el procesamiento del lenguaje natural. (Naciones Unidas : Oficina de las Naciones Unidas Contra la Droga y el Delito En México, 2023, pág. 1)

Es ciertamente positivo implementar la tecnología actual para avanzar en problemas socialmente relevantes, como lo es la violencia contra la mujer, además de ser un problema que va en constante aumento, siendo así que la innovación tecnológica se considera un gran avance para promover la eficiencia del sistema de justicia. Si bien, este sistema se realiza en México, es un ejemplo claro que se puede practicar a nivel global, siempre y cuando se cuente con lo necesario para realizar esta implementación.

Es más, también se resalta que:

El equipo del CdE UNODC-INEGI cuenta con las capacidades técnicas y metodológicas para ofrecer el apoyo al Estado Mexicano y demás países de Latinoamérica y el Caribe en la revisión de procesos y análisis de información para prevenir y atender la violencia basada en género mediante el uso de IA. (Naciones Unidas : Oficina de las Naciones Unidas Contra la Droga y el Delito En México, 2023, pág. 1)

Es importante definir que, este equipo derivado de la ONU, hace uso de la Inteligencia Artificial enfocándose en prevenir y abordar la violencia de género, y demuestra cómo la tecnología puede ser una herramienta poderosa para enfrentar problemas sociales complejos, mejorando la seguridad y el bienestar en la sociedad.

Otro ejemplo del uso beneficioso de la Inteligencia Artificial es en la prevención e investigación del tráfico ilícito de migrantes, en donde hoy en día se utiliza esta tecnología para ayudar a contrarrestar este problema. La Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2020) afirma que:

En la esfera del tráfico ilícito de migrantes, por ejemplo, esto incluye estrategias de implantación de sistemas basados en la inteligencia artificial que pueden ayudar a verificar a los viajeros en los pasos fronterizos. El enfoque basado en la inteligencia artificial permite aprovechar la capacidad de procesar e intercambiar un volumen

notable de datos en un plazo breve con el fin de generar evaluaciones completas de las amenazas y transmitir las con rapidez. (Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, 2020, pág. 8)

Aquí sin duda se puede ver como un uso responsable de la Inteligencia Artificial puede significar un avance significativo de las tecnologías actuales, el uso ético de esta herramienta puede traer consigo un sinnúmero de beneficios por su gran agilidad para realizar tareas de forma automática, pero lamentablemente no es lo que se ve mayoritariamente, es por tal motivo que se debe promover su uso ético y fomentar su regulación.

En Colombia se ha establecido el uso de la Inteligencia Artificial como ayuda importante para el sistema judicial, para entrar en contexto debo referirme a lo que determinan Gutiérrez y Flores acerca de esta valiosa información:

Un trabajo conjunto entre el Laboratorio de Innovación e Inteligencia Artificial, de la Facultad de Derecho de la Universidad de Buenos Aires, el Ministerio Público Fiscal de la Ciudad de Buenos Aires y la Universidad del Rosario de Colombia, quienes crean una herramienta que combina Inteligencia Artificial, asistencia Inteligente, automatización y Blockchain. Dicha Inteligencia Artificial da como resultado el aplicativo que hoy en día conocemos como Prometea. (Gutiérrez, 2020, pág. 57)

Es aquí donde vemos como la Inteligencia Artificial es significativa en cualquier ámbito, esta herramienta usada con el fin de disminuir de alguna manera el tiempo dentro del sistema judicial, y promover la celeridad procesal. Y se puede evidenciar que de la cooperación entre países pueden surgir mecanismos valiosos para ayudar a la ciudadanía en general.

Brevemente es preciso mencionar que “Prometea” es una herramienta de Inteligencia Artificial que según Lucía Bellocchio, representante de la CIDH, se utiliza en tres tipos de procedimientos: “para la resolución del fondo de asistencia legal a las víctimas, para realizar notificaciones a los países que forman parte de la Organización de los Estados Americanos (OEA) y como herramienta de búsqueda para rastrear precedentes.” (Luna, 2017, pág. 1)

La herramienta de inteligencia artificial "Prometea" ha demostrado ser una innovación significativa en el ámbito legal, esta aplicación multifacética de la inteligencia artificial subraya el potencial de la tecnología para mejorar la eficiencia y la precisión en procesos legales

complejos, facilitando la labor de los profesionales del derecho y beneficiando a las víctimas al acelerar los procedimientos y garantizar una mayor coherencia en las decisiones jurídicas.

Definitivamente, la inteligencia artificial ha transformado numerosos sectores, proporcionando beneficios significativos. No obstante, junto a estos avances, también surgen riesgos asociados a su implementación. Por ello, es fundamental abordar estos desafíos con regulaciones adecuadas y un enfoque ético en el desarrollo y uso de la inteligencia artificial, asegurando así que su impacto sea beneficioso y equitativo para toda la sociedad.

4.2.2. Riesgos de la Inteligencia Artificial

La Inteligencia Artificial está en un auge evidente, es indispensable relacionarnos con este asunto y conocer el alcance que tiene en diversas áreas.

La Organización de las Naciones Unidas establece que:

El sector educativo no está preparado para la integración ética y pedagógica de estas herramientas en rápida evolución. De acuerdo con una encuesta hecha por la UNESCO en más de 450 escuelas y universidades, menos del 10% cuentan con políticas institucionales o directrices formales relativas al uso de aplicaciones de inteligencia artificial generativa, en gran parte debido a la ausencia de normativas nacionales. (ONU, 2023)

Los riesgos asociados al uso desmedido de la Inteligencia Artificial es un problema real, que afecta a personas de todas las edades, desde estudiantes que pueden depender excesivamente de estas herramientas, comprometiendo su capacidad de aprendizaje crítico, hasta educadores que se enfrentan a desafíos éticos y pedagógicos al incorporar tecnologías avanzadas sin una guía clara. Esta situación subraya la urgencia de desarrollar políticas y directrices que aseguren un uso responsable y beneficioso de la inteligencia artificial en la educación.

El diario digital expreso nos pone a consideración las palabras de su entrevistado, el ingeniero en informática y experto en ciberseguridad Deepak Daswani quien establece que “la IA lleva muchos años en funcionamiento, pero su auge actual se debe a la accesibilidad para el uso masivo. Esto es particularmente relevante en áreas como las fake news, deepfakes y estafas” (González, 2024, pág. 1) Esto ejemplifica el grave riesgo que implica el mal uso de esta tecnología, que lamentablemente se ha diversificado y posicionado como un problema sin

precedentes, intensificado por la falta de un marco regulatorio claro que dificulta su adecuada gestión.

4.2.3. Regulación de la Inteligencia Artificial

El 13 de marzo de 2024, el Parlamento Europeo aprobó la primera ley en el mundo diseñada para regular la Inteligencia Artificial dentro de la Unión Europea. Es un reglamento de Inteligencia Artificial que promueve la innovación tecnológica con límites que aseguran la ética y la seguridad de estas nuevas tecnologías.

Dentro de los considerandos del Reglamento de Inteligencia Artificial del Parlamento Europeo, se establece que:

(69) El derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. (Parlamento Europeo, 2024, pág. 69)

La referencia al derecho a la intimidad y la protección de datos en el Reglamento de Inteligencia Artificial del Parlamento Europeo subraya la importancia de asegurar estos derechos a lo largo de todo el ciclo de vida de los sistemas de Inteligencia Artificial. Esto refleja un compromiso claro con la protección de datos, y sobre todo que se proteja el derecho fundamental como lo es la intimidad, y demás derechos que se puedan ver vulnerados.

El Artículo 3 del Reglamento de Inteligencia Artificial del Parlamento Europeo dictamina:

A los efectos del presente Reglamento, se entenderá por:

- 1) «sistema de IA»: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales. (Parlamento Europeo, 2024, pág. 166)

Este artículo define claramente qué se considera un sistema de Inteligencia Artificial. Esta habilidad para prever, crear contenidos, ofrecer recomendaciones o tomar decisiones puede tener un efecto importante en entornos reales y virtuales, subrayando la variedad de usos y posibles efectos de la Inteligencia Artificial en nuestra sociedad actual.

En México existe una regulación a la Inteligencia Artificial, que se encuentra dentro del Código Penal del Estado de Sinaloa, el mismo que identifica acertadamente la definición de Inteligencia Artificial. El Código Penal del Estado de Sinaloa define: “Art.185 Bis C.- Se entenderá por Inteligencia Artificial las aplicaciones, programas o tecnología que analice fotografías, audios o videos y ofrece ajustes automáticos para hacerles alteraciones o modificaciones.” (Código Penal del Estado de Sinaloa, 1992, pág. 71). En este contexto, la importancia de tipificar este delito en nuestro sistema jurídico, es esencial para abordar con urgencia esta problemática y su impacto en la sociedad.

4.3. Terminología Informática

La informática abarca una amplia gama de conceptos y términos que son fundamentales en todo lo que comprende el entorno digital, mismo que se encuentra en constante evolución, cada término tiene su propia relevancia y aplicación en la tecnología moderna, y analizar cada uno de ellos es de gran importancia para entender los conceptos que abarca la Inteligencia Artificial.

4.3.1. Deepfakes

Laura Payne, escritora contribuyente para la Enciclopedia Británica nos da una descripción del término Deepfakes, término inglés que adaptado al español sería falsedades profundas: “Deepfakes, medios sintéticos, que incluyen imágenes, videos y audio, generados por tecnología de inteligencia artificial (IA) que retratan algo que no existe en la realidad o eventos que nunca han ocurrido” (Payne , 2024, pág. 1). Es necesario destacar el gran aporte que nos presenta esta autora, debido a que, hoy en día es común encontrar en las redes sociales una serie infinita de noticias falsas, conocidas comúnmente como fake news, perdiendo así la autenticidad de la información que se comparte actualmente. De hecho, por llamar la atención de los usuarios, muchas personas optan por popularizar Deepfakes constantemente y así viralizar contenidos falsos que afectan a quienes se ven involucrados.

Es importante comprender que este tipo de contenido, vulnera directamente la intimidad de las personas, puesto que, quien se encuentre afectado por estas manipulaciones sufrirá injerencias

sobre sí mismo, opiniones sobre un contenido falso en el que se manipuló y deshonró su imagen afectando sus derechos sin poder protegerse de ello, porque ¿cómo puede defenderse sin una norma clara que lo ampare?.

Payne también conceptualiza de forma general el objetivo de los Deepfakes, como señala a continuación:

Los Deepfakes, en la mayoría de los casos, están asociados con motivos nefastos, incluida la creación de información errónea y la generación de confusión sobre asuntos políticamente importantes. Se han utilizado para degradar, intimidar y acosar y no sólo se han dirigido a celebridades, políticos y directores ejecutivos, sino también a ciudadanos comunes y corrientes. (Payne , 2024, pág. 1)

Con este criterio se comprende que este tipo de contenido creado por personas inescrupulosas es una realidad y cada vez se encuentra más extendido globalmente, y sobre todo hoy en día que existe la facilidad de remitir este tipo de información por todo el mundo de manera considerablemente rápida, debido al uso de las redes sociales y el avance de la tecnología en el aspecto de la comunicación.

La Constitución de la República del Ecuador estipula que:

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. (Asamblea Constituyente, 2008, pág. 12)

Este artículo constitucional enfatiza claramente la importancia que tiene la información verídica sobre los hechos ocurridos, contribuyendo al forjamiento de una sociedad bien informada. En el contexto actual, los Deepfakes pueden distorsionar la realidad y socavar la confianza pública, es fundamental que se proteja el derecho a la información auténtica. Además, la proliferación de Deepfakes es una amenaza tangible que requiere una respuesta inmediata tanto desde el marco legal como desde la educación pública. Siendo así que, la misma Constitución nos garantiza a todos los ciudadanos el debido acceso a información confiable .

4.3.2. Machine Learning

El Diccionario sobre Inteligencia Artificial define al machine learning o aprendizaje automático en español, como:

Un componente fundamental de la inteligencia artificial que permite a las máquinas aprender patrones y mejorar su rendimiento sin intervención humana explícita. Utiliza algoritmos que permiten a las máquinas reconocer patrones en datos y tomar decisiones basadas en estos patrones, mejorando su desempeño con la experiencia. (TN University , 2024, pág. 5)

El machine learning se define como un proceso mediante el cual los dispositivos tecnológicos realizan tareas aprendiendo grandes cantidades de datos, de forma automática. Y es fundamental en el desarrollo de las nuevas tecnologías como lo es la Inteligencia Artificial, y se aplica en una diversidad de áreas. También permite una capacidad de autoaprendizaje realmente innovadora, transformando significativamente la forma en que interactuamos con la tecnología hoy en día.

La investigadora de la Universidad de Cuenca Johanna Orellana Alvear define que:

El aprendizaje automático, o más conocido como “machine learning”, se basa en las ciencias de la computación, ciencia de datos y estadística. Esta sub-área de la IA, utiliza observaciones del mundo real y permite a las computadoras (o más explícitamente a un algoritmo), identificar patrones a partir de esos datos. (Orellana, 2024, pág. 1)

El machine learning, es una disciplina que se fundamenta en las ciencias de la computación, datos y estadística. Usando observaciones del mundo real para permitir que las computadoras, a través de algoritmos, identifiquen patrones y este proceso mejora continuamente la capacidad de los ordenadores para tomar decisiones y realizar tareas de manera autónoma, lo que resulta una evolución significativa en múltiples aplicaciones tecnológicas. De hecho, esta subárea de la Inteligencia Artificial debería de enseñarse dentro de las instituciones educativas para con ello fortalecer la educación en todo lo respecta a las nuevas tecnologías.

La Constitución de la República del Ecuador determina que:

Art. 347.- Será responsabilidad del Estado:

8. Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales. (Asamblea Constituyente, 2008, pág. 129)

Es la propia Constitución de la República del Ecuador quien establece como responsabilidad del Estado, implementar dentro del ámbito educativo las tecnologías de la información y comunicación, en este caso, estas subáreas de la Inteligencia Artificial son de gran ayuda para que dentro del sistema de educación se instauren nuevos procesos de aprendizaje sobre la tecnología que se desarrolla continuamente y a gran medida.

4.3.3. Deep Learning

En el Diccionario sobre Inteligencia Artificial se define todo lo referente al Deep Learning, añadiendo que:

También conocido como aprendizaje profundo, es un subcampo del aprendizaje automático que se basa en redes neuronales artificiales para realizar tareas complejas de procesamiento de datos. A diferencia de los modelos de aprendizaje automático tradicionales, que pueden tener una o dos capas ocultas, las redes neuronales profundas pueden tener múltiples capas ocultas, lo que les permite aprender representaciones jerárquicas de los datos. Esto hace que el Deep learning sea especialmente eficaz en tareas como reconocimiento de imágenes, procesamiento de lenguaje natural y reconocimiento de voz. (TN University , 2024, pág. 8)

Este transcendental diccionario de terminología utilizada en lo concerniente a Inteligencia Artificial, determina la importancia del aprendizaje profundo para el desarrollo de la misma, y se puede conocer sobre la capacidad que tienen algunos dispositivos electrónicos para aprender y adaptarse de manera similar al cerebro humano, lo cual determina un avance significativo en diversas áreas, siempre y cuando se maneje con responsabilidad y ética.

Como podemos observar, este término informático se refiere a la capacidad que pueden tener los dispositivos tecnológicos de aprender muchos datos y posteriormente realicen tareas similares a los humanos. Un ejemplo de ello son los asistentes virtuales en nuestros teléfonos, como Siri, o Asistente de Google, también son destacables los prácticos dispositivos como Alexa, o el sistema de Chat GPT, en donde con una sola pregunta se puede tener una vasta información sobre algún tema, incluso puede simular una conversación con otro humano,

ilustrando de esta manera la capacidad de aprendizaje automático. Estos sistemas responden a nuestras preguntas, reproducen música que le pidan, nos brindan información sobre el clima, nos ayudan a gestionar tareas cotidianas como enviar mensajes o realizar llamadas de forma automática, siendo un avance tecnológico realmente importante.

El Deep Learning “permite configurar parámetros básicos relacionados con datos e información, y capacitar a una computadora para que aprenda por sí misma” (Da Silva y otros, 2021, pág. 1), con ello se puede determinar que las computadoras pueden identificar patrones complejos y hacer predicciones precisas sin intervención humana constante. Sin embargo, esta capacidad también plantea desafíos significativos en términos de ética y seguridad, especialmente cuando se utiliza para manipular información, como en el caso de los Deepfakes, donde se manipulan archivos de video, imagen y voz para crear un contenido realista pero completamente falso.

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos dictamina que:

“Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia”

En el contexto del comercio electrónico, el Deep learning debe cumplir con los principios de confidencialidad y reserva según lo establece la Ley de Comercio, Electrónico, Firmas y Mensajes de Datos, esto asegura que el uso de tecnologías avanzadas se enmarque dentro de nuestra legislación para determinar su uso ético y en cumplimiento de la normativa vigente, la tecnología Deep learning puede ser considerada como parte de esta ley, ya que implica el uso de algoritmos y sistemas informáticos avanzados para el procesamiento y análisis de datos. En síntesis, refuerza la confianza de los usuarios y empresas en las transacciones electrónicas y el manejo de información.

4.3.4. Algoritmo

Según la Real Academia de la Lengua Española, un algoritmo es: “Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema”. (RAE, 2024, pág. 1) Este término en el ámbito informático, es básicamente aquellas instrucciones o pasos que se usan

para resolver una tarea específica, son la base de la programación y la informática puesto que, guían a las computadoras en la ejecución de diversas operaciones. Son fundamentales en la resolución de problemas y en el diseño de sistemas y aplicaciones informáticas, ya que permiten automatizar tareas y optimizar procesos.

4.3.5. Deepfaces y Deepvoices.

Son un tipo de Deepfakes que, mediante el uso de la Inteligencia artificial, se encargan de generar, en el caso de Deepfaces imágenes aparentemente reales sin serlo, que, por medio del aprendizaje automático de la inteligencia artificial, se manipulan y se generan nuevas imágenes o vídeos a partir de otros. Y por otra parte los Deepvoices se encargan de suplantar la voz de una persona en un audio, haciendo que parezca verídico, es decir, se realiza una falsificación de voz.

El experto en seguridad de la firma ESET, Jake Moore, explicó a Forbes que:

La manipulación del audio, más fácil de orquestar que la realización de vídeos de Deepfakes, sólo va a aumentar en volumen. Sin la educación y la conciencia de este nuevo tipo de ataque, junto con mejores métodos de autenticación, es probable que más empresas sean víctimas de conversaciones falsificadas muy convincentes. De hecho, basta con que la voz de alguien esté disponible en Internet para que sea posible reproducirla y manipularla con tecnologías de voz de inteligencia artificial. (Biurrun, 2021, pág. 1)

En nuestro país, hemos observado en la red social X, anteriormente conocida como Twitter, la circulación de audios aparentemente filtrados de figuras públicas, en los cuales se expresan comentarios negativos sobre el país o situaciones controversiales. Aunque posteriormente estas personas han declarado que se trata de Deepfakes, el daño a su credibilidad ya ha sido causado. La facilidad con la que se produce falsificaciones de voz utilizando la Inteligencia Artificial es extremadamente desarrollada, además de ser una violación a la intimidad, también se produce un daño severo al honor y buen nombre.

4.3.6. Ciberespacio

La Real Academia Española define al ciberespacio como aquel “ámbito virtual creado por medios informáticos.” (Real Academia Española, 2001, pág. 1) Por este motivo, se debe

considerar al ciberespacio como aquel entorno digital donde transitan la información, las aplicaciones, las comunicaciones y todo lo que respecta al contenido que se encuentra dentro de medios digitales.

Marisa Avogadro para la Revista Electrónica en América Latina Especializada en Comunicación nos menciona que “El ciberespacio es el nuevo medio de comunicación que surge de la interconexión mundial de los sistemas de datos. Incluye la infraestructura material de la información digital y el universo de informaciones que contiene.” (Avogadro M. , 2012, pág. 1)

En la vida diaria, el término ciberespacio se utiliza ampliamente para describir el entorno digital en el que interactuamos, accedemos a información, nos comunicamos y realizamos transacciones en línea. Refleja la importancia de Internet y la digitalización en nuestra vida cotidiana, destacando cómo ha transformado la manera en que vivimos, trabajamos, nos comunicamos y nos relacionamos con el mundo.

4.4. Entorno Digital

4.4.1. Redes sociales

Las Redes sociales son parte de nuestro diario vivir, es el medio donde transita la información que consumimos día a día, aunque nos puede ser de gran utilidad para comunicarnos, informarnos, etc., también se debe considerar los riesgos que estas plataformas conllevan.

Podemos definir a las redes sociales como aquellas “plataformas digitales formadas por comunidades de individuos con intereses, actividades o relaciones en común (como amistad, parentesco, trabajo). Las redes sociales permiten el contacto entre personas y funcionan como un medio para comunicarse e intercambiar información.” (Equipo editorial, Etecé, 2023, pág. 1)

Si bien las redes sociales son una herramienta importante en nuestro día a día, que entre sus múltiples funciones está el de comunicarnos, también ha sido parte de esta difusión desenfadada de información falsa, que afecta a personas de todas las edades. Si bien algunas redes sociales tienen una edad mínima para acceder, hoy en día vemos que desde niños utilizan estas plataformas de interacción, debido a falta de limitaciones por parte de sus progenitores.

Al respecto, es importante tener en cuenta que, al compartir contenido en las redes sociales, los usuarios aceptan una serie de términos y condiciones, y de acuerdo a esas políticas de seguridad, la persona al aceptar, estaría consintiendo que su información se haga pública y accesible globalmente, es aquí donde se genera el problema, ya que esto puede generar conflictos en donde los derechos de los ciudadanos se vean afectados. Las redes sociales más comunes son: Instagram, X, Facebook, Tiktok, sitios donde usualmente los usuarios publican imágenes o videos de sí mismos, de sus familiares o de su entorno en general, exponiendo este contenido a la manipulación mediante el uso la Inteligencia Artificial, y consecuentemente exista una vulneración a su intimidad.

4.4.2. Medios cibernéticos

Los medios cibernéticos, también conocidos como medios digitales, son plataformas y herramientas que utilizan tecnologías digitales para crear, distribuir y consumir contenido. Es importante conocer lo que la doctrina nos establece al respecto.

Maryalejandra Montiel analiza el ámbito informático y señala que los Medios Cibernéticos:

Son aquellos que vienen de la edición impresa o audiovisual y emergen dentro de estas tecnologías, pero se ubican en el ciberespacio apoyados por recursos tecnológicos e informáticos donde se une el medio impreso y el audiovisual, además de desarrollar posibilidades de hipervínculos (texto, sonido, video e imágenes) y ser interactivos. (Montiel, 2000, pág. 44)

La autora básicamente nos indica que los Medios Cibernéticos son una evolución de los medios tradicionales, como la edición impresa y audiovisual, que han migrado al ciberespacio y se apoyan en recursos tecnológicos e informáticos. Estos medios combinan elementos del medio impreso y audiovisual, ofreciendo posibilidades de hipervínculos y siendo interactivos, lo que significa que permiten la participación activa del usuario.

4.4.3. Cibercriminos

En nuestro país, se ha establecido la UNIDAD NACIONAL ESPECIALIZADA EN INVESTIGACIÓN DE CIBERDELITO, conforme a la Resolución No. 34-FGE-2022 emitida por la Fiscalía General del Estado, la cual se encuentra vigente en el Registro Oficial desde el

17 de junio de 2022. Esta unidad especializada fue creada con el propósito de llevar a cabo investigaciones y acciones fiscales sobre los delitos informáticos tipificados en el COIP.

Pero ¿qué entendemos por ciberdelitos?, para poder tener una idea clara sobre este término, me pareció necesario implementar la definición que Avogadro da a los ciberdelitos o también llamados delitos informáticos, mencionando que son “(...) las actividades ilegales en las que intervienen medios electrónicos y nuevas tecnologías” (Avogadro M. , 2009, pág. 1) Estos delitos son un problema existente y de gran relevancia en la actualidad, la interconexión global ha permitido que los ciberdelincuentes operen a escala nacional e internacional, aprovechando la falta de fronteras físicas y la dificultad para rastrear sus actividades, puesto que, estos delitos son cometidos en su mayoría por individuos que se encuentran en el extranjero.

En países como Chile, Argentina, Perú, México, así como en lugares con avances tecnológicos evidentemente rápidos como lo son Estados Unidos y Europa, la tipificación de los ciberdelitos es una realidad y cada día se adaptan al desarrollo tecnológico y nuevos mecanismos desarrollados con el fin de cometer delitos. Estas regulaciones reflejan el esfuerzo global por adaptar la legislación a los desafíos y avances tecnológicos actuales.

4.5. Manipulación digital de archivos de video, imagen o voz

4.5.1. Origen de la manipulación digital de archivos de video, imagen o voz

La edición de videos, imágenes o voz es una práctica que se ha llevado a cabo durante muchos años, es importante reconocer el origen de esta técnica y destacar la contribución del Técnico Especialista en Comunicación, Guillermo López Aliaga, quien nos señala que “en este repaso por el origen del montaje, el nacimiento del video, a partir de los años cincuenta, el cual comenzó con tecnología analógica también y posteriormente en los noventa, dio el salto al mundo digital” (Aliaga, 2021, pág. 7) La evolución de la edición desde sus comienzos en los años cincuenta hasta la transición al mundo digital en los noventa muestra el continuo avance y adaptación de las tecnologías de comunicación. Hoy en día, cualquier persona con un dispositivo electrónico puede editar videos, imágenes o voces con relativa facilidad.

La revolución digital en los años noventa, cuando la accesibilidad a Internet creció significativamente, marcó el inicio de una era de desarrollo tecnológico, sentando las bases para la transformación digital que se puede evidenciar en el actual siglo XXI. Pasamos de editar videos pegando o cortando partes y añadiendo efectos de sonido, a la era de la Inteligencia

Artificial, cuya manipulación de archivos de video, imagen o voz mediante su uso ha ganado mucha popularidad por su rápida difusión en internet. La Inteligencia Artificial realiza esta manipulación con un alto grado de realismo, superando las técnicas convencionales, los resultados de tal manipulación son extremadamente convincentes.

La Ley de Comunicación establece que: “Art.22.- Todas las personas tienen derecho a que la información de relevancia pública que reciben a través de los medios de comunicación sea verificada, contrastada, precisa y contextualizada (...)” (Asamblea constituyente, 2013, pág. 8). Este derecho resalta la importancia de garantizar el derecho que tienen los ciudadanos a recibir información confiable, el derecho a la verdad, teniendo en consideración la calidad y la veracidad de la información que se difunde en los medios, sobre todo hoy en día que la difusión de información por internet se ha masivado, este derecho también se vulnera en un contexto donde la manipulación de archivos digitales mediante la Inteligencia Artificial se use para difundir información falsa o engañosa.

4.5.2. Herramientas utilizadas en la manipulación digital de archivos de video, imagen o voz

Para la manipulación de aquellos archivos de video, de imagen y de voz se han creado herramientas para su fácil acceso y mediante el uso de la Inteligencia Artificial, estas herramientas se han popularizado por su rápido resultado de edición y realismo.

El profesor e investigador Dr. Jorge Franganillo, nos comenta que fue “a lo largo de 2022 que se popularizó la creación de imágenes a partir de texto gracias a herramientas como Craiyon, DALL·E, Midjourney y Stable Diffusion.” (Franganillo, 2023, pág. 7) Estos datos logran determinar que dichas aplicaciones tienen la capacidad de inventar ilustraciones innovadoras de toda índole. Para lo cual, utilizan sistemas de Inteligencia Artificial mediante Deep learning a partir de mucha información. Sin embargo, esto supone la creación de imágenes a partir de texto, pero la manipulación va más allá.

A continuación, se detallan algunas herramientas que utilizan Inteligencia Artificial para la creación de Deepfakes, y las manipulaciones que constituyen un riesgo a la intimidad de las personas en todos sus aspectos.

4.5.2.1. D-ID

Dentro de lo respecta a la manipulación de videos, imágenes o voz; se identifica a la aplicación pagada que usa inteligencia artificial llamada D-ID, la cual no necesita de conocimientos técnicos para su uso, de hecho, su facilidad de creación de videos a partir de texto permite a los usuarios hacerlo en pocos minutos, permite crear videos realistas a partir de fotos estáticas, utilizando tecnología avanzada de IA para animar imágenes faciales y convertirlas en videos.

El Ingeniero Informático Mario Granero establece que “D-ID se diferencia de otras aplicaciones de creación de videos en que utiliza inteligencia artificial para generar videos de alta calidad a partir de texto simple” (Granero, 2023, pág. 1). Estas herramientas están revolucionando la industria del entretenimiento, la publicidad y la educación, pero también plantean preocupaciones sobre el uso indebido, como la creación de Deepfakes para desinformar o manipular, y más aún por la facilidad de acceso que tienen los usuarios.

4.5.2.2. DeepFaceLab

El desarrollo y la disponibilidad de software como DeepFaceLab ha transformado el campo de la edición de videos, imágenes y voz, permitiendo la creación de Deepfakes con un grado de realismo sin precedentes.

Weitzman, se refiere a este software de la siguiente forma:

DeepFaceLab es un software de Deepfakes de código abierto que funciona en ordenadores Windows. Es una de las herramientas más potentes en este campo y utiliza algoritmos de aprendizaje automático y aceleración por GPU para crear vídeos falsos de alta calidad. (Weitzman, 2024, pág. 1)

El autor destaca la potencia de DeepFaceLab como una herramienta de código abierto que, a través de algoritmos de aprendizaje automático, permite generar videos falsos de alta calidad. Este avance tecnológico plantea desafíos significativos en términos de ética y seguridad digital, puesto que, a facilidad con la que se pueden crear estos Deepfakes subraya la necesidad urgente de establecer regulaciones para evitar el abuso de estas herramientas y la desinformación como consecuencia de su mal uso.

4.5.2.3. FaceApp

En el mundo de la edición digital, las aplicaciones basadas en inteligencia artificial han revolucionado la manera en que interactuamos con nuestras imágenes. Otro ejemplo destacado de esta tendencia es FaceApp, que ha ganado popularidad por su capacidad de modificar imágenes de manera realista y efectiva. “FaceApp puede añadir sonrisas, cambiar el género de una persona y aumentar o reducir tu edad con sus filtros fotorrealistas. Esta aplicación usa redes neuronales de inteligencia artificial que logran personalizar cualquier selfie como si fuera tu Photoshop privado” (University of Advanced Technologies, 2019, pág. 1)

Es así que esta tecnología tiene la capacidad de manipular una imagen a tal punto que se perciba completamente real, el realismo evidencia una gran utilidad en el entorno del marketing, pero representa un problema cuando las intenciones se derivan de personas poco éticas y con la intención de dañar la imagen de alguien más.

4.5.2.4. ZAO

ZAO es una aplicación que se popularizó debido a su originalidad, y uso de Inteligencia Artificial, el proceso según se describe en el diario Primicias es el siguiente: “Los consumidores se inscriben en ZAO con su número de teléfono y suben imágenes de su cara, utilizando fotografías tomadas con su smartphone. A continuación, pueden elegir entre una serie de vídeos de celebridades en los que superponer su rostro” (Redacción Primicias / EFE, 2019, pág. 1). Esta aplicación ha captado la atención del público por su innovador uso de la inteligencia artificial para la creación de Deepfakes, permitiendo a los usuarios colocar sus propios rostros en videos de celebridades, lo que genera resultados impactantes y realistas. Según el diario Primicias, el proceso es simple: los usuarios se registran, suben una foto de su rostro y seleccionan el video en el que desean aparecer. Esta accesibilidad de uso ha contribuido significativamente a su popularidad.

Sin embargo, el hecho de permitir el uso de su imagen genera un peligro inminente ante mal utilización de su imagen. El periódico digital Primicias también establece que “Una sección del acuerdo de usuario establece que los consumidores que suben sus imágenes a ZAO aceptan ceder los derechos de propiedad intelectual a su cara, y permiten a ZAO utilizar sus imágenes con fines de marketing” (Redacción Primicias / EFE, 2019, pág. 1). Esto es realmente importante destacar, puesto que hoy por hoy, con el acceso a redes sociales, las personas usualmente aceptan los términos y condiciones sin leer que, en su mayoría, los términos

consisten en conceder el acceso a su imagen. Esta práctica puede llevar a posibles violaciones de la privacidad e intimidad de las personas, siendo fundamental que los usuarios sean conscientes de los riesgos y lean detenidamente los acuerdos de usuario para proteger sus derechos de imagen.

En el ámbito legal, es importante destacar que en la Constitución de la República del Ecuador decreta:

Art. 66.- Se reconoce y garantizará a las personas:

7. El derecho de toda persona que ha sido agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario. (Asamblea Constituyente, 2008, pág. 26)

Este artículo estima la reparación en caso de difusión de información falsa por medios de comunicación social, sin embargo, es importante saber que en caso de que una persona haya sido agraviada por manipulación de videos, imágenes o voz sobre sí mismo, sería equivalente a información falsa, el presente artículo también se

Además, el COIP determina un tipo penal relacionado a la manipulación de archivos:

Art.103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años. (Asamblea Constituyente, COIP, 2014, pág. 37)

Se consideró pertinente citar este artículo debido a que aborda un delito informático que involucra el término edite. Sin embargo, es importante tener en cuenta que editar y manipular no son sinónimos. Además, es relevante destacar que este delito informático podría incluir la manipulación de archivos multimedia con propósitos de pornografía infantil. Y cabe mencionar que este artículo fue reformado en su primer inciso, el 30 de agosto de 2021, con el objetivo de

prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos.

En España, el derecho a la propia imagen está protegido principalmente por la Constitución Española, la cual establece que: “Artículo 18 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen” (Constitución Española, 1978, pág. 16). Si bien en nuestro país el derecho a la intimidad y el derecho al honor y al buen nombre están debidamente reconocidos por la Constitución, la Constitución Española también reconoce el derecho a la propia imagen, lo cual es fundamental, puesto que este derecho protege a las personas contra el uso no autorizado de su imagen y garantiza su dignidad y autonomía. Además, en un contexto donde las redes sociales y las nuevas tecnologías están siempre presentes, la protección de la propia imagen se vuelve aún más relevante, ya que ayuda a prevenir abusos y vulneraciones que pueden afectar gravemente a la sociedad.

4.6. Derecho a la Intimidad Personal y Familiar

La intimidad personal y familiar es un derecho fundamental que garantiza la protección de la esfera privada de las personas y de sus relaciones. En este punto abordaré detalladamente desde una perspectiva jurídica y doctrinaria los aspectos relacionados con la intimidad.

El Diccionario de Derecho Procesal Constitucional y Convencional, define el derecho a la intimidad de la siguiente forma:

Así, el derecho a la intimidad tiene la función de proteger, frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar, aquella información que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. (Ferrer y otros, 2014, pág. 351)

Este Diccionario describe el derecho a la intimidad como una protección contra cualquier intromisión en la vida personal y familiar de una persona. Esta protección abarca tanto la información que una persona desea mantener privada como las intrusiones de terceros que se realizan sin su consentimiento. Esta definición subraya la importancia de preservar un espacio personal libre de invasiones externas, asegurando que cada individuo tenga control sobre qué aspectos de su vida son accesibles a otros.

La Dra. María Bibiana Nieto, conjuntamente con la Dra. María Inés Montesano manifiestan respecto al derecho a la intimidad que:

El derecho a la intimidad es el derecho humano fundamental que permite a las personas mantener ciertos ámbitos de su vida personal y familiar a resguardo de la publicidad y de intromisiones arbitrarias de terceros. Este derecho abarca lo que comúnmente se denomina “vida privada” que incluye lo íntimo, lo personal, lo familiar y algunos aspectos de los ámbitos social y laboral. (Nieto, 2016, pág. 2)

La Dra. María Bibiana Nieto y la Dra. María Inés Montesano destacan la importancia del derecho a la intimidad como un derecho humano fundamental. Este derecho protege a las personas, permitiéndoles mantener ciertos aspectos de su vida personal y familiar alejados del escrutinio público y de las intromisiones arbitrarias de terceros. Según las autoras, la intimidad abarca no solo la vida privada en términos íntimos y personales, sino también los ámbitos familiar, social y laboral. Esta protección es clave para preservar la dignidad y autonomía de los individuos en diversos contextos de su vida cotidiana, además de preservar la seguridad jurídica que se encuentra establecida en nuestra Carta Magna.

El derecho a la intimidad personal y familiar se encuentra debidamente protegido por la Constitución de la República del Ecuador, en el Capítulo Sexto sobre los Derechos de libertad, establece que: “Art. 66.- Se reconoce y garantizará a las personas: 20. El derecho a la intimidad personal y familiar.” (Asamblea Constituyente, 2008, pág. 26). Siendo un motivo determinante para establecer a la intimidad como un derecho fundamental, que debe ser protegido rigurosamente en todos los ámbitos de la vida social y legal. Este derecho asegura a los individuos el control sobre su información personal, resguardando su dignidad y autonomía frente a intervenciones indebidas o invasivas.

A más de ello, es preciso destacar lo que establece el Código Orgánico Integral Penal, acerca de la intimidad personal y familiar, dictaminando que:

Art. 5.- Principios procesales.- El derecho al debido proceso penal, sin perjuicio de otros establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, se regirá por los siguientes principios: 10. Intimidad: toda persona tiene derecho a su intimidad personal y familiar. No podrán hacerse registros, allanamientos, incautaciones en su domicilio, residencia o lugar de trabajo, sino en virtud de orden de la o el juzgador competente, con arreglo a las

formalidades y motivos previamente definidos, salvo los casos de excepción previstos en este Código.

Además de ser un derecho fundamental, es un principio por el que se deberá regir el derecho al debido proceso penal, asegurando que cualquier actuación que afecte la intimidad personal y familiar de una persona se realice conforme a estrictos criterios judiciales, es decir, bajo un orden expresa de la autoridad competente.

Es importante identificar que, dentro del Código Orgánico Integral Penal, Capítulo Segundo, Delitos contra los Derechos de Libertad, Sección Sexta, Delitos contra el Derecho a la Intimidad Personal y Familiar, se encuentra tipificado el tipo penal de Violación a la intimidad, dictaminando que:

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. (Código Orgánico Integral Penal, 2014, pág. 59)

El empleo de la Inteligencia Artificial para la manipulación de archivos multimedia con propósitos poco éticos constituye una forma contemporánea de violación del derecho a la intimidad. Esta manipulación genera contenido falso que representa una vulnerabilidad evidente, especialmente si no se aborda legalmente la amenaza que surge a medida que esta tecnología avanza sin un marco legal adecuado. Aunque el derecho a la intimidad personal y familiar está definido legalmente, el cuerpo legal vigente contempla una serie de acciones específicas, como: acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar; sin considerar explícitamente la manipulación de archivos. No obstante, es esencial que el verbo rector "manipular" también se incluya en este tipo penal, ya que el uso de la Inteligencia Artificial para alterar contenido también vulnera el derecho a la intimidad.

La Declaración Universal de los Derechos Humanos expresa que:

Art. 12.- Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. (Declaración Universal de Derechos Humanos, 1948, pág. 3)

Este reconocimiento global del derecho a la intimidad personal y familiar enfatiza la importancia de este principio fundamental. En un mundo donde la tecnología puede representar una amenaza para la intimidad, estas garantías legales cobran aún más relevancia, destacando la necesidad de su respeto y aplicación rigurosa en la sociedad.

En el ámbito jurídico, se destaca el poder que tienen las personas para controlar su círculo íntimo, personal y familiar, permitiéndoles excluir a extraños de interferir en él y evitar una divulgación no deseada. Esta concepción resalta la importancia del derecho a la intimidad como un derecho fundamental, que en la actualidad se ve constantemente vulnerado por los avances tecnológicos, es determinante poder reconocer y sobre todo proteger este derecho desde todas sus dimensiones.

El Código Penal de Sinaloa en el Capítulo V BIS, referente a la Violación de la intimidad sexual, establece que:

ARTÍCULO 185 Bis C. Comete el delito de violación a la intimidad sexual, aquella persona que por cualquier medio publique, divulgue, difunda, comparta o distribuya imágenes, vídeos o audios, imprima o elabore textos de contenido íntimo sexual de una persona sin su consentimiento expreso, voluntario, genuino y deseado. Esta conducta se sancionará con una pena de tres a seis años de prisión y de quinientos a mil días multa. Se presume que se publica, divulga, difunde, comparte o distribuye contenidos íntimos de naturaleza sexual cuando se trate de imágenes o videos que muestren al sujeto pasivo en situación de desnudez parcial o total, o con exposición de partes genitales. Se presume que se publica, divulga, difunda, comparte o distribuye audios o textos con contenido íntimo sexual cuando en ellos se describa el cuerpo desnudo ya sea total o parcialmente del sujeto pasivo; o bien que revelen de manera no autorizada ni expresamente consentida la conducta o actos sexuales de la víctima. (Honorable Congreso del Estado de Sinaloa, 1992, pág. 71)

Sin embargo, el 12 de febrero de 2024, se aprobó una reforma de ley a este artículo en el que se añadió lo siguiente:

Se impondrán las mismas penas previstas en el segundo párrafo del presente artículo, a quien haciendo uso de la Inteligencia Artificial, manipule imágenes, audios o videos, de contenido íntimo sexual de una persona, para crear hechos falsos con apariencia real, con el propósito de exponer, distribuir, difundir, exhibir, reproducir, transmitir, comercializar, ofertar, intercambiar y/o compartir a través de materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier otro medio tecnológico, sin su consentimiento expreso, voluntario, genuino y deseado. (Honorable Congreso del Estado de Sinaloa, 1992, pág. 71)

Esta reforma legal busca proteger primordialmente la intimidad, consciente de que la difusión de contenido sexual falso puede causar un profundo daño psicológico y emocional a las víctimas, así como perjudicar su reputación. Este caso ilustra cómo herramientas como la Inteligencia Artificial pueden ser penalizadas debido a su capacidad para manipular fotos, videos y audios, violando así el derecho a la intimidad. La reforma refleja cómo se están considerando estas tecnologías en la vulneración de derechos fundamentales, dado que la Inteligencia Artificial puede manipular estos archivos con un realismo que vulnera completamente la intimidad de las personas y su entorno.

4.7. El Delito

Es importante describir lo que es el delito, su etimología, como está consagrado doctrinariamente, y por supuesto, su determinación en la ley.

El diccionario de la Corte Interamericana de Derechos Humanos define al delito como:

Etimológicamente, la palabra delito proviene de la similar latina "delictum", aun cuando en la técnica romana poseyera significados genuinos, dentro de una coincidente expresión calificadora de un hecho antijurídico y doloso sancionado con una pena. (Corte Interamericana de los Derechos Humanos, 2023, pág. 1)

Esta definición subraya la naturaleza delictiva de un acto no solo por su carácter antijurídico, es decir, contrario a la ley, sino también por su componente doloso, lo que implica la intención o el conocimiento de cometer un acto ilícito.

El delito como lo menciona el Dr. Ernesto Albán Gómez: “es un ente de hecho, un acto del hombre, un fenómeno natural y social, producido por factores endógenos y exógenos de la

persona, ya sea antropológicos, psíquicos o sociales...” (Albán Gómez, 2018) La definición del Dr. Ernesto Albán destaca la complejidad y la naturaleza multifacética del delito al considerar que varios factores pueden influir en su ocurrencia. Al mencionar aspectos antropológicos, psíquicos y sociales, esta definición reconoce que el delito es el resultado de una interacción compleja entre el individuo y su entorno. Analizar el delito requiere una comprensión profunda de todo lo que contribuye al cometimiento del delito.

El reconocido jurista Francesco Carrara, citado por Ernesto Albán, menciona que: “Delito es la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, y que resulta de un acto externo del hombre, positivo o negativo, moralmente imputable y socialmente dañoso”. (Albán Gómez, 2018) Carrara enfatiza la relación del delito y la ley. Al describir el delito como una infracción de la ley destinada a proteger la seguridad de los ciudadanos, se resalta la necesidad de un marco legal claro y de la responsabilidad individual en el cumplimiento de las normas sociales.

El delito se encuentra descrito como infracción penal en el Código Orgánico Integral Penal, estableciendo que: “Art. 18.- Infracción penal.- Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código.” En síntesis, el delito es aquella conducta que cumple con lo que establece el tipo penal y por lo tanto debe ser sancionada, y de hecho el mismo cuerpo legal dictamina que las infracciones penales se clasifican tanto en delitos como en contravenciones.

4.7.1. Estructura del delito

4.8.1.1. Conducta:

El reconocido jurista español Manuel Ossorio proporciona la siguiente definición de conducta: “Modo de proceder una persona, manera de regir su vida y acciones” (Ossorio, 2008, pág. 195), dicha definición es acertada y encapsula el comportamiento humano en términos generales, el autor destaca que la conducta abarca las acciones individuales de la persona y aquel conjunto de normas y principios que guían dichas acciones, es decir, la forma en que una persona lleva a cabo su vida.

El catedrático penalista Claus Roxin destaca que “Derecho penal se compone de la suma de todos los preceptos que regulan los presupuestos o consecuencias de una conducta conminada con una pena o con una medida de seguridad y corrección.” (Roxin, 1997, pág. 41), el autor

destaca que el derecho penal incluye todas las normas que regulan cuándo una conducta es castigada, y es pertinente subrayar que la conducta penalizada es el elemento clave del Derecho penal, mismo que, no solo se enfoca en castigar, sino también en prevenir y corregir comportamientos.

El Código Orgánico Integral Penal dispone que: “Art. 22.- Son penalmente relevantes las acciones u omisiones que ponen en peligro o producen resultados lesivos, descriptibles y demostrables” (Código Orgánico Integral Penal, 2014)

Es así que, en nuestro marco legal se determina que inicialmente se debe verificar que sea una conducta punible, es decir, que haya existido acción u omisión, con repercusiones desfavorables. Este enfoque asegura que la penalización se base en hechos concretos y verificables, evitando sanciones arbitrarias.

Sin embargo, hay situaciones donde una conducta ilícita no es penalizada, nuestro Código Penal determina exactamente ese tipo de circunstancias: “Art. 24.- Causas de exclusión de la conducta.- No son penalmente relevantes los resultados dañosos o peligrosos resultantes de fuerza física irresistible, movimientos reflejos o estados de plena inconciencia, debidamente comprobados.” (Asamblea Constituyente, COIP, 2014, pág. 14) El presente artículo aborda importantes excepciones en la penalización de conductas ilícitas, estableciendo que no se consideran penalmente relevantes los daños o peligros resultantes de circunstancias como fuerza física irresistible, movimientos reflejos o estados de inconciencia, siempre que estas situaciones sean debidamente comprobadas. Este enfoque destaca la importancia de la intención y la conciencia del individuo al determinar la relevancia penal de una conducta.

4.8.1.2. Tipicidad:

La tipicidad en el contexto legal se refiere a la adecuación de una acción específica a un tipo de delito establecido por la ley, son aquellas acciones que no cumplen con los criterios que establece la ley, es decir, aquellas que no están contempladas en el catálogo de delitos independientemente de su carácter antijurídico o culpable.

Cabanellas citando a Jiménez de Asúa expresa que:

La vida diaria nos presenta una serie de hechos contrarios a la norma y que por dañar la convivencia social se sancionan con una pena, estando definidos por el código o las

leyes, para poder castíganos. Esa descripción legal, desprovista de carácter valorativo, es lo que constituye la tipicidad. (Cabanellas, 2006, pág. 461)

Esta definición que nos destaca el jurista, garantiza que solo se castiguen los actos que están claramente descritos en la ley. Aunque puede ser un poco objetivo, se considera que esto ayuda a asegurar que el sistema de justicia sea eficiente, ya que solo se sancionan los comportamientos que están bien definidos y establecidos en el código penal, así, se evitaría que las personas sean castigadas por actos que no están claramente definidos como delitos.

Cuando hablamos del principio de tipicidad, entendemos que para que un hecho consumado sea típico, una ley debe preverlo, no importa la forma o manera que se lo haga, se entiende a la tipicidad como un elemento del delito que consta en una estrecha relación de la adecuación al tipo penal, entre un hecho de la vida real a lo que se tipifique en el tipo penal; estas acciones se pueden realizar por medio de acciones u omisiones, que la ley considere delictivos. (Bonilla, et al., 2021, pág. 3)

El principio de tipicidad garantiza que para que un acto sea considerado un delito, debe estar claramente definido en la ley. Esto significa que cualquier hecho que se considere delictivo debe encajar con precisión en la descripción legal del tipo pena, siendo así que, la tipicidad es fundamental dentro del derecho penal, pues establece la correspondencia entre una acción y un tipo delictivo definido por la ley, garantizando la certeza jurídica al delimitar claramente qué comportamientos son punibles y cuáles no lo son.

Dentro del Código Orgánico Integral Penal se determina a la tipicidad como: “Art. 25.- Tipicidad.- Los tipos penales describen los elementos de las conductas penalmente relevantes.” (Asamblea Constituyente, COIP, 2014, pág. 15). Y básicamente, se encuentra establecida la tipicidad como un concepto claro que adecúa la conducta al tipo penal establecido, es decir que dicha conducta tipificada debe ser tal y como se describe en la ley para que pueda recibir una sanción.

En el contexto de la tipicidad se encuentran establecidas las formas en las que no exista infracción penal para asegurar la objetividad de la sanción.

Nuestro Código Orgánico Integral Penal estrictamente determina que:

Art. 28.1.- Error de tipo.- No existe infracción penal cuando, por error o ignorancia invencibles debidamente comprobados, se desconocen uno o varios de los elementos objetivos del tipo penal. Si el error es vencible, la infracción persiste y responde por la modalidad culposa del tipo penal, si aquella existe. El error invencible que recae sobre una circunstancia agravante o sobre un hecho que califique la infracción, impide la apreciación de esta por parte de las juezas y jueces. (Asamblea Constituyente, COIP, 2014, pág. 15)

Este enfoque dentro de nuestra normativa protege a quienes desconocen ciertos elementos objetivos del tipo penal, sin embargo, si el error es vencible, la infracción sigue existiendo y se califica de manera culposa. Así se busca equilibrar la justicia al distinguir errores que se pueden suscitar para el cometimiento del delito, y se asegura que sean penalizadas las conductas en donde haya plena responsabilidad.

4.8.1.3. Antijuridicidad:

La antijuridicidad es un concepto central en el derecho penal que se refiere a la característica de un acto que contraviene las normas jurídicas vigentes, pues determina si una conducta, al ser contraria al ordenamiento legal, debe ser considerada como un delito. Es por ello que es importante comprender la antijuridicidad para identificar qué acciones son punibles en el marco de la ley.

El ilustre abogado Guillermo Cabanellas establece que la antijuridicidad es: “Elemento esencial del delito, cuya formula es el valor que se concede al fin perseguido por la acción criminal en contradicción con aquel otro garantizado por el Derecho.” (Cabanellas, 2006, pág. 26), La definición contenida en el diccionario jurídico subraya la importancia de examinar el conflicto entre el objetivo de la acción criminal y los valores protegidos por el Derecho, destacando así su importancia como un elemento fundamental del delito.

Para comprender más a fondo lo que es la antijuridicidad es pertinente señalar lo que el Dr. Juan Bustos, manifiesta: “La antijuridicidad tiene un carácter material y formal y por consiguiente la afección a un bien jurídico y su imputación objetiva al hecho típico, resultan aspectos fundamentales y anteriores a resolver si existen o no causas de justificación.” (Bustos, 2004, pág. 7). En sus palabras, el autor destaca la importancia de considerar tanto la dimensión material como formal de la antijuridicidad. Subrayando que la afectación a un bien jurídico y su

imputación objetiva al hecho tipificado son aspectos de suma importancia que deben abordarse antes de determinar si existen circunstancias que justifiquen la conducta.

El Código Orgánico Integral Penal delimita a la antijuricidad como: “Art. 29.- Antijuricidad.- Para que la conducta penalmente relevante sea antijurídica deberá amenazar o lesionar, sin justa causa, un bien jurídico protegido por este Código.” (Asamblea Constituyente, COIP, 2014, pág. 15) Es por ello que, en este concepto se destaca que no solamente es necesario que se adecúe la conducta en el tipo penal, si no que, además, la conducta debe ser considerada antijurídica, es decir, debe lesionar un bien jurídico, debe vulnerar un derecho, debe estar prohibida por el ordenamiento jurídico establecido.

El Código Orgánico Integral Penal define:

Art. 30.- Causas de exclusión de la antijuricidad.- No existe infracción penal cuando la conducta típica se encuentra justificada por estado de necesidad o legítima defensa.

Tampoco existe infracción penal cuando se actúa en cumplimiento de una orden legítima y expresa de autoridad competente o de un deber legal, debidamente comprobados. (Asamblea Constituyente, COIP, 2014, pág. 16)

Este artículo reconoce que ciertas acciones, aunque técnicamente delictivas, pueden ser justificables y no punibles cuando se realizan bajo circunstancias permitidas por la ley, y por lo tanto para determinar que un hecho delictivo debe penalizarse se debe evaluar el contexto y las razones detrás de la conducta para así poder determinar su antijuricidad.

En síntesis, la antijuricidad es un factor determinante en el derecho penal, puesto que define cuándo una conducta contraviene las normas jurídicas y, por ende, puede considerarse un delito. Por lo tanto, la correcta determinación de la antijuricidad asegura que solo se sancionen conductas que verdaderamente contravengan el ordenamiento jurídico, más no aquellas que se hayan realizado por motivos que la ley exceptúe.

4.8.1.4. Culpabilidad:

La RAE determina que la culpabilidad es el “último gran elemento o requisito del delito como presupuesto de la pena que permite la atribución personal del hecho al sujeto activo, autor o partícipe, del mismo” (RAE, 2024, pág. 1) La culpabilidad tiene como fundamento que para que una persona sea considerada responsable penalmente deberá ser imputable y actuar con

conocimiento de la antijuridicidad de su conducta, para ello el Código Orgánico Integral Penal determina que no existirá responsabilidad penal en los casos de error de prohibición invencible y trastorno mental, debidamente comprobados.

Acerca de la culpabilidad, el destacable jurista Claus Roxin expone: “También el principio de culpabilidad se encuentra en íntima relación con el de legalidad, pues no se podría reprochar su conducta a quien no pudo conocer con anterioridad a la misma que estaba prohibida penalmente.” (Roxin, et al., 1989, pág. 36), el destacado doctor resalta que el principio de culpabilidad está estrechamente vinculado al principio de legalidad, indicando que no se puede imputar responsabilidad penal a alguien que no tenía forma de saber que su conducta estaba prohibida. Esta observación destaca la importancia de la previsibilidad en el derecho penal asegurando que solo sean responsabilizadas las personas que la ley determine como culpables.

En nuestra normativa interna, el Código Orgánico Integral Penal define a la culpabilidad como: “Art. 34.- Culpabilidad.- Para que una persona sea considerada responsable penalmente deberá ser imputable y actuar con conocimiento de la antijuridicidad de su conducta” (Asamblea Constituyente, COIP, 2014, pág. 17) Según lo expuesto, además de ser una conducta típica y antijurídica se debe considerar el último elemento de suma importancia que es la culpabilidad, básicamente la culpabilidad se refiere a la capacidad del sujeto para comprender la ilicitud de su comportamiento y actuar conforme a esa comprensión, se analiza si el sujeto tenía la intención de cometer el acto delictivo y si comprendía las consecuencias de sus acciones.

Finalmente, es factible mencionar que, existen casos que, una conducta puede ser típica y antijurídica pero no logra concretarse el elemento de culpabilidad por razones que nuestro CÓDIGO Orgánico Integral Penal dictamina: “Art. 35.- Causas de inculpabilidad.- No existe responsabilidad penal en los casos de error de prohibición invencible y trastorno mental, debidamente comprobados.” (Asamblea Constituyente, COIP, 2014, pág. 17) Según el ordenamiento jurídico de nuestro país, la ausencia de responsabilidad penal puede darse en dos situaciones, error de prohibición invencible o trastorno mental, siempre que estos factores sean debidamente justificados y verificados, garantizando que no se penalice a quienes, debido a estas circunstancias, no deben ser considerados responsables de sus actos ante la ley.

En conclusión, para que una conducta sea punible, debe ser típica, antijurídica, y el autor, además, debe ser culpable. Solo cuando se cumplan todos estos requisitos, la conducta se considera un delito y puede dar lugar a una sanción, pero siempre y cuando se cumpla con

todos sus elementos, esto significa que no solo se debe determinar si el acto infringe la ley, sino también si el individuo actuó con conocimiento y voluntad, y evidentemente que no deben existir razones que justificaran su conducta.

5. Metodología

5.1. Materiales Utilizados.

Durante el desarrollo del presente Trabajo de Integración Curricular es fundamental reconocer los materiales que usé, y que hicieron posible el cumplimiento de los objetivos presentados, los cuales son: Libros, diccionarios jurídicos, manuales, revistas científicas, artículos científicos, leyes. Y especialmente sitios web de diversas instituciones judiciales tanto a nivel internacional como local, los cuales he referenciado de manera organizada junto con sus fuentes bibliográficas. Además de los materiales previamente mencionados, también usé otros recursos como complemento para el desarrollo del presente trabajo.: Cuaderno de apuntes, teléfono celular, computadora, impresora, conexión a internet.

5.2. Métodos

En el transcurso de la presente investigación, se emplearon diversos métodos para la obtención de resultados, los cuales se detallan a continuación:

Método Inductivo: El método científico se basó en la observación de casos específicos para llegar a una conclusión general. Es por ello, que con el uso de este método busqué datos detallados para comprender el origen, beneficios, riesgos y regulación de la Inteligencia Artificial, para determinar la necesidad de una reforma al artículo 178 Del Código Orgánico Integral Penal.

Método Deductivo: El método deductivo implicó partir de principios generales para llegar a conclusiones específicas. En mi investigación, lo apliqué para analizar si la manipulación de archivos multimedia mediante el uso de la Inteligencia Artificial afecta principalmente el derecho a la intimidad personal y familiar, concluyendo que sí y que además produce afectaciones a otros derechos como lo son, el honor y buen nombre, la protección de datos de carácter personal y el derecho a la verdad.

Método Hermenéutico: El método hermenéutico se basa en la interpretación y el análisis crítico para extraer significados más allá de la superficie literal, explorando las intenciones,

valores y contextos. En el ámbito de la presente investigación, utilicé este método para el análisis de artículos, revistas y obras científicas que desarrollé en el Marco Teórico.

Método Comparativo: El método comparativo es una aproximación en la investigación que consiste en analizar similitudes y diferencias entre dos o más elementos. En este trabajo, apliqué el método comparativo para analizar el Derecho Comparado, contrastando la realidad jurídica de Ecuador con el Código Penal del Estado de Sinaloa en México y la Unión Europea. Además, se examinaron casos de manipulación de videos, imágenes y voz tanto a nivel nacional como internacional.

5.3. Técnicas

Para la ejecución del presente Trabajo de Integración Curricular se emplearon las siguientes técnicas:

Técnicas de acopio teórico documental: Permitió la realización del marco teórico para un mejor aporte y desarrollo del trabajo mediante información actualizada y verídica, por medio de la selección de información de datos bibliográficos y documentales.

Técnicas de acopio empírico: Se conocen como técnicas de campo:

- **Encuesta:** Para aplicar esta técnica, se llevó a cabo un formulario de encuestas con preguntas claras y concretas, dirigidas a 30 profesionales del Derecho y especialistas en informática, con el fin de obtener respuestas y recolectar datos. Una vez tabulados, se pudo conocer la opinión pública sobre la problemática planteada.
- **Entrevista:** Esta técnica se basó en la realización de preguntas con la ayuda de un formulario de entrevistas y equipo celular para la grabación, fue realizada a 5 profesionales del Derecho y especialistas en informática, quienes respondieron acerca de aspectos concretos del tema de investigación, y sus respuestas fueron fundamentales para la obtención de información relevante acerca de la problemática planteada.

6. Resultados.

6.1. Resultados de Encuestas.

La presente técnica de la encuesta fue aplicada a treinta profesionales del Derecho y especialistas en informática de la ciudad de Loja. El cuestionario está conformado por seis preguntas, de las cuales se obtuvieron los siguientes resultados que a continuación son presentados.

Primera pregunta:

¿Estima usted que con la manipulación de archivos de video, imagen o voz mediante la Inteligencia Artificial se afecta principalmente?:

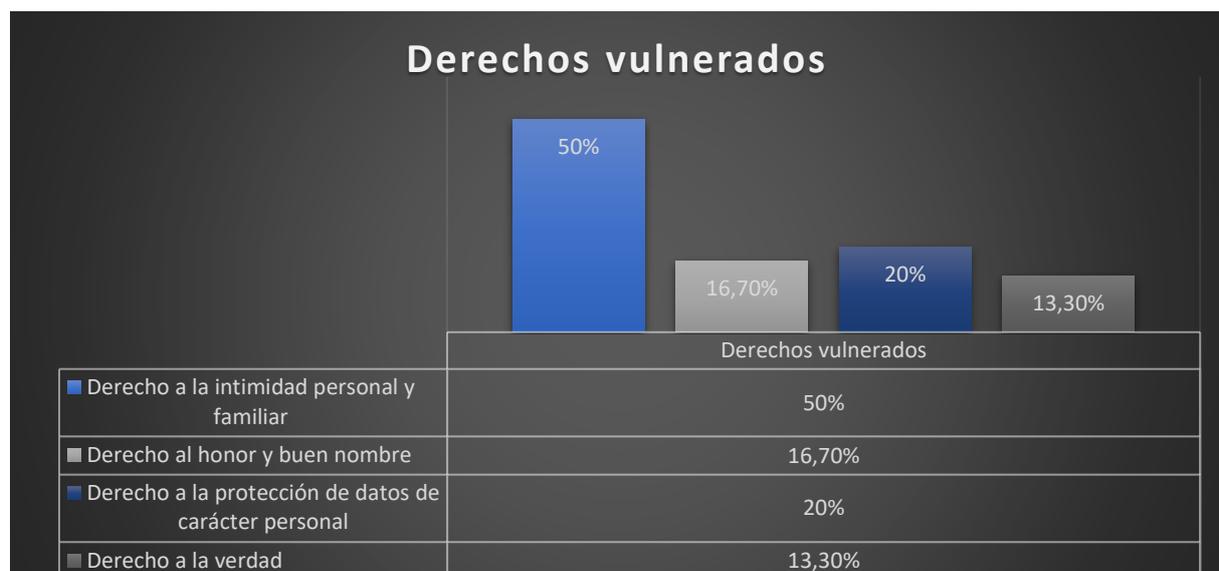
Tabla Nro. 1.

Indicadores	Variables	Porcentaje
Derecho a la intimidad personal y familiar	15	50%
Derecho al honor y buen nombre	5	16.70 %
Derecho a la protección de datos de carácter personal	6	20%
Derecho a la verdad	4	13,30%
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja.

Autora: Evelyn del Carmen Vargas Granda.

Figura Nro. 1.



Interpretación:

En la presente pregunta se obtuvo los siguientes resultados, 15 de los 30 encuestados, que corresponden al 50% indicaron que el derecho que más se vulnera por la manipulación de archivos de video, imagen o voz por el uso indebido de la Inteligencia Artificial es el derecho a la intimidad personal y familiar; por otro lado, 5 encuestados que representan el 16,70% señalaron el derecho a al honor y buen nombre; mientras que, 6 encuestados, que simbolizan el 20% señalan la vulneración del derecho a la a la protección de datos de carácter personal; y, finalmente, 4 encuestados, que figuran el 13,30% indican que por la falta de una política criminal contra la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial se vulnera el derecho a la verdad.

Análisis

En la presente pregunta se obtuvo una variedad de respuestas, de lo cual puedo manifestar que la mayoría de los encuestados indicaron que el derecho que más se ve afectado debido a la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial es el derecho a la intimidad personal y familiar. Estoy de acuerdo con este criterio, ya que, desde mi perspectiva, este derecho constitucionalmente protegido tiene como finalidad que las personas disfruten de su vida privada sin interferencias externas, en este sentido, la difusión de imágenes, videos o audios falsos, generados por Inteligencia Artificial y presentados como reales, sin el consentimiento del individuo, vulnera gravemente el derecho a la intimidad, tanto a nivel personal como familiar, pues cada persona tiene el derecho de exigir respeto no solo en sus acciones como individuo, sino también como miembro integrante de un núcleo familiar. Sin embargo, y en concordancia con la doctrina, este fenómeno no se limita solo a la vulneración de la intimidad, puesto que, se podría considerar como un delito pluriofensivo, es decir, que afecta a múltiples derechos simultáneamente.

Segunda Pregunta:

¿Cree usted que el uso de la Inteligencia Artificial en la manipulación archivos de video, imagen o voz afecta gravemente el derecho a la intimidad personal y familiar?

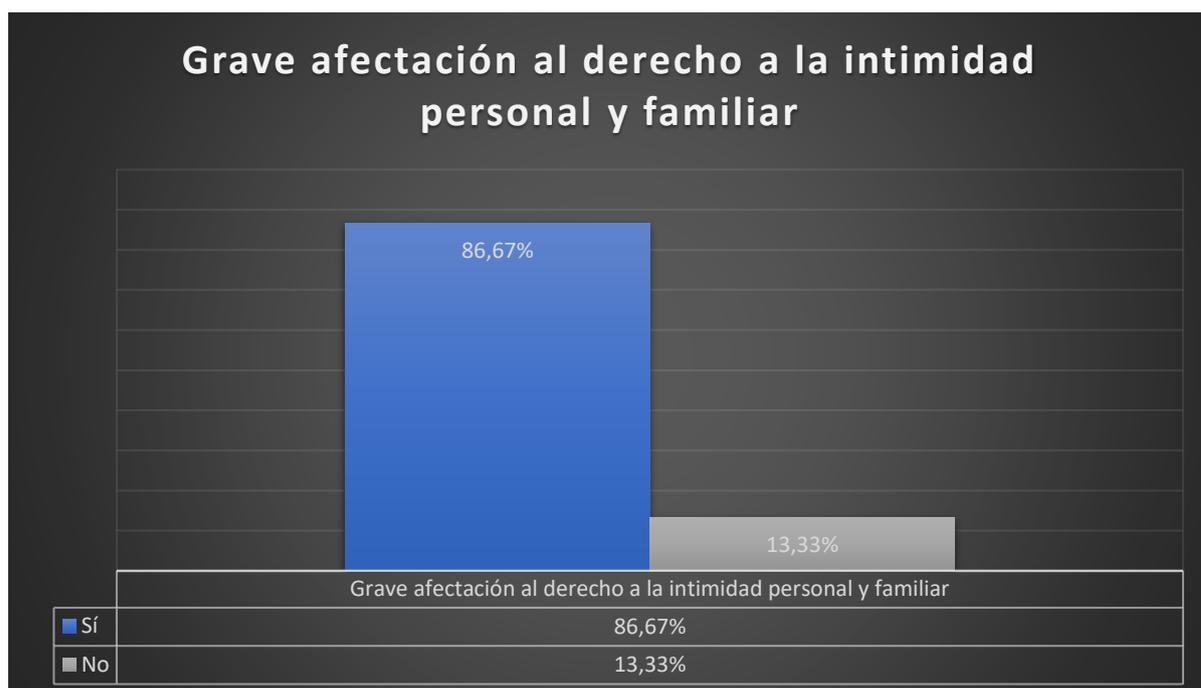
Tabla Nro. 2.

Indicadores	Variables	Porcentaje
Sí	26	86,67%
No	4	13,33 %
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja.

Autora: Evelyn del Carmen Vargas Granda.

Figura Nro. 2.



Interpretación:

En la presente pregunta se obtuvo los siguientes resultados, 26 de los 30 encuestados, que corresponden al 86,67% manifestaron que el uso de la Inteligencia Artificial en la manipulación de archivos de video, imagen o voz sí afecta gravemente el derecho a la intimidad personal y familiar. Estos encuestados consideran que la tecnología, cuando se usa para crear contenido

multimedia falso, puede tener consecuencias devastadoras en la vida personal de los individuos. Además, resaltan la necesidad de establecer regulaciones claras y efectivas para proteger este derecho fundamental. Por otro lado, cuatro 4 de los encuestados que representan el 13,33% señalan que el uso de la Inteligencia Artificial en la manipulación de archivos de video, imagen o voz no afecta gravemente el derecho a la intimidad personal y familiar. Estos encuestados creen que, aunque la tecnología puede ser utilizada de manera indebida, no consideran que su impacto sea lo suficientemente significativo como para vulnerar gravemente este derecho.

Análisis:

En lo que respecta a esta pregunta, coincido con la mayoría de los profesionales encuestados, los cuales consideran que en el Ecuador no existe una política bien definida para abordar los problemas derivados del mal uso de la Inteligencia Artificial. Señalando, que el uso de esta tecnología afecta gravemente el derecho a la intimidad personal y familiar, preocupación evidentemente válida, ya que actualmente en nuestro país la regulación y las políticas preventivas para este tipo de manipulaciones digitales son inexistentes. Es fundamental que el Estado ecuatoriano desarrolle e implemente una política estructurada que no solo contemple la penalización de los delitos derivados del uso indebido de la Inteligencia Artificial, sino que también incluya programas de educación y concienciación sobre los riesgos y las consecuencias de estas tecnologías y debe ser ampliamente conocida y comprendida por la población para garantizar su efectividad.

En este contexto, la precaria situación de las políticas actuales refleja la necesidad de un enfoque más integral y proactivo que incluya la participación de diversas instituciones y la sociedad en su conjunto. Esto es esencial para mitigar el impacto negativo de la manipulación de archivos de video, imagen y voz, y para proteger los derechos fundamentales de los ciudadanos, especialmente el derecho a la intimidad personal y familiar.

Tercera pregunta:

¿Estima usted que la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar?

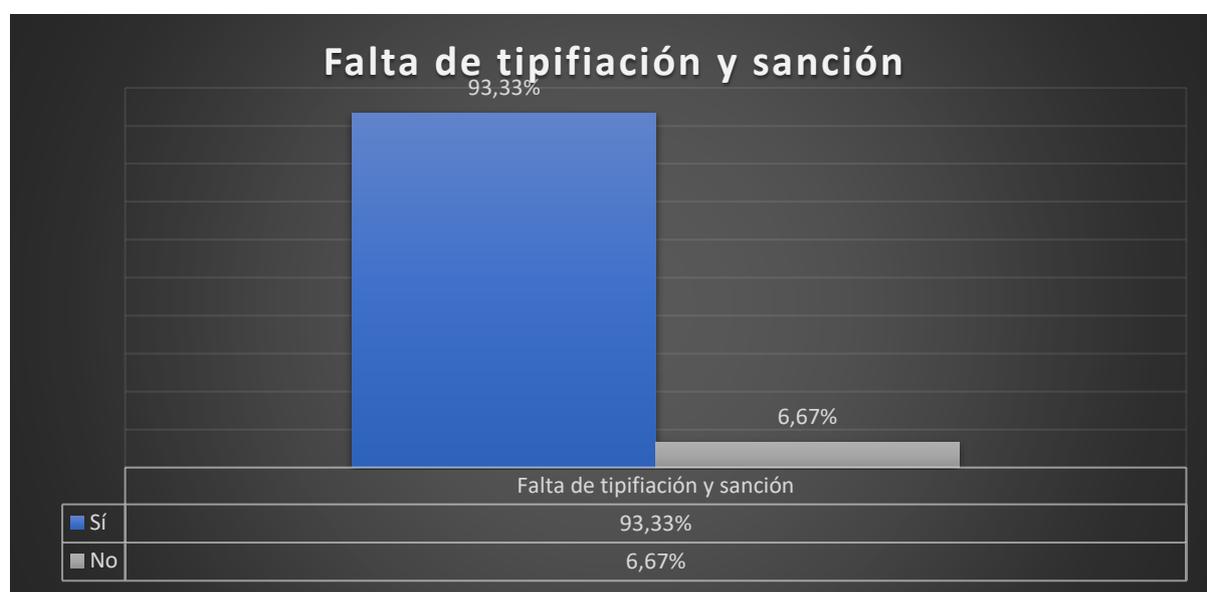
Tabla Nro. 3.

Indicadores	Variables	Porcentaje
Sí	28	93,33%
No	2	6,67 %
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja.

Autora: Evelyn del Carmen Vargas Granda.

Figura Nro. 3.



Interpretación:

En la presente pregunta, 28 de los 30 encuestados que corresponden al 93,33% indicaron que la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar. Por su parte 2 de los encuestados correspondiente al 6,67 % no consideran que haya

vulneración a la intimidad personal y familiar como consecuencia de la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial. Basándonos en la situación actual de nuestro país, podemos concluir que el Estado no está garantizando una correcta seguridad ciudadana, ya que la criminalidad en el país va en aumento y la ausencia de una política clara y definida para abordar este tipo de delitos cibernéticos deja una brecha significativa en la protección de los derechos fundamentales de los ciudadanos.

Análisis:

En la presente pregunta, comparto la opinión de la mayoría de los encuestados, los cuales manifestaron que la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar. Este resultado pone de manifiesto una preocupación generalizada sobre la capacidad del Estado para proteger derechos fundamentales en el contexto de nuevas tecnologías y basándonos en la situación actual de nuestro país, la falta de medidas preventivas y la ausencia de una legislación específica que tipifique y sancione adecuadamente la manipulación de archivos mediante Inteligencia Artificial muestra una deficiencia en la estructura legal del Estado.

La encuesta muestra que la vulneración del derecho a la intimidad personal y familiar es una preocupación crítica que requiere una acción inmediata y coordinada por parte del Estado y la sociedad para establecer un marco legal efectivo y bien definido que proteja estos derechos en el contexto de la tecnología moderna.

Cuarta pregunta:

¿Está usted de acuerdo en tipificar y sancionar en la legislación penal ecuatoriana la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial para garantizar el derecho a la intimidad personal y familiar?

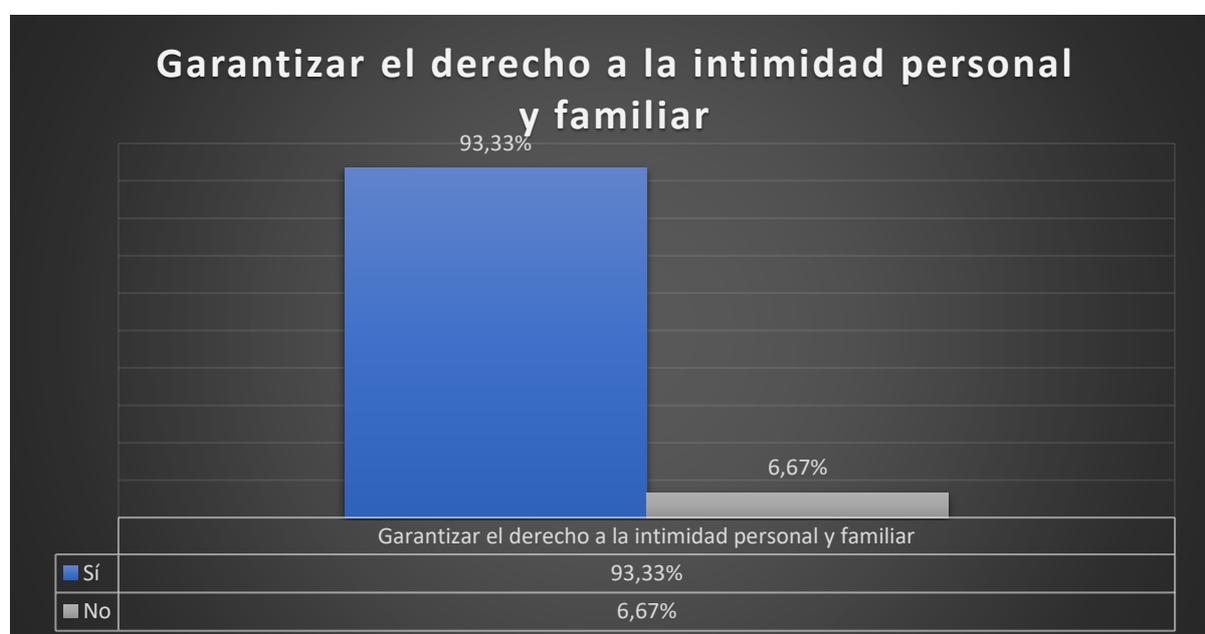
Tabla Nro. 4.

Indicadores	Variables	Porcentaje
Sí	28	93,33%
No	2	6,67 %
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja.

Autora: Evelyn del Carmen Vargas Granda.

Figura Nro. 4.



Interpretación:

En la presente pregunta, 28 de los 30 encuestados, que corresponden al 93,33%, indicaron de manera mayoritaria que sí están de acuerdo con la tipificación y sanción en la legislación penal ecuatoriana de la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial para garantizar el derecho a la intimidad personal y familiar. Considerando que la inclusión de estas medidas en el marco legal proporcionará una eficiente protección contra el abuso de estas tecnologías. Mientras tanto, 2 de los encuestados, representando el 6,67%, manifestaron que no están de acuerdo, fundamentando que la

penalización puede no ser la solución más efectiva y una mejor alternativa sería algo menos restrictivo como la regulación tecnológica, la educación pública y las medidas preventivas.

Análisis:

Estoy de acuerdo con el resultado de estas respuestas, que revela una división de opiniones entre los encuestados. Mientras la mayoría sostiene que la penalización es necesaria para garantizar la protección frente al abuso de tecnologías de Inteligencia Artificial que afectan la privacidad personal y familiar, una minoría aboga por enfoques más flexibles y educativos. Esta discrepancia subraya la complejidad del tema y la necesidad de considerar diferentes perspectivas al diseñar políticas y legislaciones relacionadas con la regulación de la tecnología y la protección de derechos fundamentales. En resumen, el alto grado de acuerdo hacia la penalización refleja una preocupación generalizada por la protección de la intimidad frente a los avances tecnológicos.

Quinta pregunta:

¿Cree usted necesario que se realicen campañas de concientización para educar a la sociedad sobre los riesgos de la manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial?

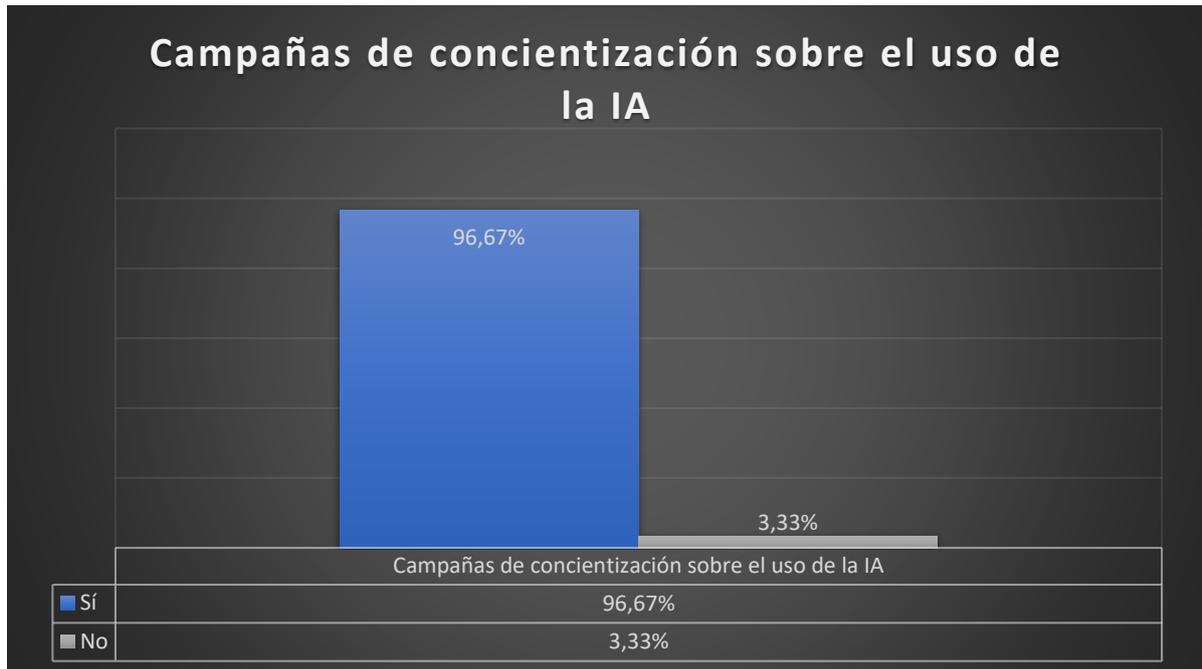
Tabla Nro. 5.

Indicadores	Variables	Porcentaje
Sí	29	96,67%
No	1	3,33 %
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja.

Autora: Evelyn del Carmen Vargas Granda.

Figura Nro. 5.



Interpretación:

En la presente pregunta, 29 de los 30 encuestados, que corresponden al 96,67%, indicaron sí es necesario que se realicen campañas de concientización para educar a la sociedad sobre los riesgos de la manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial, de manera mayoritaria están de acuerdo. Mientras tanto, 1 de los encuestados, representando el 3,33%, manifiesta que generalmente este tipo de campañas suelen tener los efectos contrarios a los que se espera, es decir, podría generar más interés por realizar esta conducta que por prevenirla.

Análisis:

En esta pregunta, comparto la opinión de la mayoría de los encuestados expresando su apoyo a la realización de campañas de concientización para educar a la sociedad sobre los riesgos asociados con la manipulación de archivos de video, imagen o voz mediante el uso de Inteligencia Artificial. Este alto porcentaje refleja una clara preocupación y reconocimiento de la importancia de informar a la población sobre los posibles peligros que pueden surgir de estas tecnologías avanzadas. Por otro lado, un pequeño pero significativo número de encuestados ha manifestado escepticismo hacia estas campañas, sugiriendo que podrían tener efectos contrarios a los objetivos previstos. Esta opinión subraya la necesidad de diseñar estrategias

educativas efectivas que no solo informen sobre los riesgos de la manipulación de IA, sino que también promuevan prácticas responsables en el uso de estas tecnologías.

En resumen, los resultados de la encuesta destacan la importancia de implementar iniciativas de concientización que puedan equilibrar la promoción de la innovación tecnológica con la protección de la intimidad y otros derechos fundamentales, asegurando así un uso ético y seguro de la Inteligencia Artificial en beneficio de la sociedad.

6.2. Resultados de las entrevistas

Para continuar con el desarrollo de las entrevistas, se formularon seis preguntas abiertas dirigidas a cinco profesionales del Derecho y especialistas en Informática de la ciudad de Loja. Las entrevistas permitieron a los entrevistados razonar y expresarse libremente, lo que resultó en la obtención de información valiosa basada en su criterio y conocimiento, enriqueciendo significativamente la investigación con sus ideas innovadoras.

Este enfoque facilitó abordar de manera óptima la problemática planteada y detectar las falencias existentes. Las entrevistas se grabaron utilizando un teléfono celular y se transcribieron en el presente documento con su debido análisis e interpretación.

Primera pregunta:

Según su criterio, ¿Cuáles son las afectaciones adicionales al derecho a la intimidad personal y familiar que se dan como consecuencia de la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial?

Respuestas:

Primer entrevistado: Estamos frente al desarrollo de las TIC y estamos hablando también de la tecnología de punta, la Inteligencia Artificial que invade no solamente la intimidad de las personas sino otras particularidades, está incursionando en todos los campos de la ciencia, del saber humano, causando afectaciones a la intimidad, privacidad, seguridad jurídica, estamos frente a una amenaza al Estado como regulador que emite las leyes para precautelar los intereses de las personas. Nuestro país está paralizado en todo aspecto y mucho más en el aspecto tecnológico. La Inteligencia Artificial está para dominarnos, no para liberarnos, por ende, el Estado ecuatoriano no tiene leyes no solamente para controlar la IA, si no para

controlar otros medios de comunicación como las redes sociales, nosotros no tenemos una comunicación real si no manipulada, tergiversando el pensamiento científico.

Segundo entrevistado: Mi caso concreto es que el 1 de abril, yo siempre uso las redes sociales para hablar con mi familia e intenté ingresar a mi Facebook y no me era permitido, decía que estaba intentando ingresar a una cuenta que no me corresponde, e hice el proceso de recuperación de contraseña y no fue posible de ninguna forma. Resulta que otra persona está usando mi cuenta, y esta persona publicaba un video como si fuese yo diciendo que invierta dinero. Recibí un curso de estrategias digitales para fortalecer las clases y entre ella nos informaron sobre el uso del D-ID, una plataforma de creación de videos generados por inteligencia artificial, teniendo poco conocimiento de tecnología compartí esta información con mis estudiantes, diciéndoles que hagan un video y se presenten, consiste en poner una foto de uno mismo y la frase que se quiere decir, y automáticamente se produce un video. Y prácticamente aprendí que el video que realizaron de mí, lo realizaron manipulando una foto mía usando la inteligencia artificial. Aunque parece sencillo darse cuenta que sea un video manipulado, personas cercanas con poco conocimiento de la tecnología cayeron tal estafa e incluso me amenazaron con denunciarme. Afectaron mi intimidad, mi privacidad, mi reputación, mi honor, y dichas afectaciones cayeron sobre mí, y sobre mi entorno que cayó en la estafa.

Tercer entrevistado: Podemos remitirnos a un contexto histórico y creo que la manipulación de video existe desde que existe registro de video, la edición de video no es algo nuevo, la Inteligencia Artificial lo ha masivado lo ha puesto a un mayor alcance. La afectación que se da en este contexto es que uno tiene derecho al buen nombre, aunque relacionemos cuestiones de video a intimidad, también hay afectaciones por ejemplo al honor y buen nombre, Hay videos realizados con Inteligencia Artificial con la intención de estafas, pero también otro tipo de videos con “animos iocandi”, que significa con intención jocosa, como por ejemplo políticos bailando o ubicando alguien fuera de contexto, considero que tiene afectaciones más allá del derecho a la intimidad por ejemplo el derecho al honor al buen nombre, derecho al desarrollo de la libre personalidad.

Cuarto entrevistado: Es de fácil acceso a los menores de edad los cuales están propensos a engaños, estafas e incluso robos. Afectando su intimidad y su privacidad.

Quinto entrevistado:

- Daño psicológico a la integridad de la persona.
- Pérdida de confianza de la información.
- Linchamiento mediático.
- Suicidios por grave daño psicológico.

Comentario de la autora:

En base a la información proporcionada, se puede concluir que el concepto de la Inteligencia Artificial es bien conocido pero sobre todo, su afectación a la intimidad personal y familiar es evidente, así como algunas afectaciones adicionales que algunos de los entrevistados destacaron en común, el primer entrevistado se enfocó en la privacidad y seguridad jurídica como afectaciones adicionales, el segundo entrevistado de igual forma determinó a la intimidad y privacidad, pero también la reputación y el honor, es importante hacer énfasis en el criterio del tercer entrevistado que manifestó su desacuerdo con la afectación a la intimidad personal y familia, pues destaca la idea de que las afectaciones que se dan realmente como consecuencia de la manipulación de archivos de video, imagen o voz usando la Inteligencia Artificial es al honor y buen nombre, y también el derecho al desarrollo de la libre personalidad. Por su parte el cuarto entrevistado comparte el criterio de anteriores entrevistado diciendo que se afecta tanto a la intimidad como la privacidad, y finalmente el quinto entrevistado proporciona una afectación importante como lo es el daño psicológico, la pérdida de confianza de la información, y el linchamiento mediático.

En base a la información proporcionada, se concluye que la inteligencia artificial tiene un impacto significativo en la intimidad personal y familiar. Los entrevistados resaltaron afectaciones adicionales como la privacidad, seguridad jurídica, reputación, honor y buen nombre, el derecho al desarrollo de la libre personalidad, daño psicológico, la pérdida de confianza en la información, y linchamiento mediático como consecuencias importantes.

Segunda pregunta:

¿Considera usted que hay vulneración a la intimidad personal y familiar como consecuencia de la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial?

Respuestas:

Primer entrevistado: Totalmente, ahora pueden manipular un video diciendo que soy yo quien habla sin embargo es completamente falso, y esto puede influir radicalmente, con la manipulación de archivos de video, imagen o voz se viola a la intimidad, mucho más en países como el nuestro que no tiene control ni conocimiento de cómo funcionan las TIC.

Segundo entrevistado: Por supuesto, se afectó mi entorno, mi familia, mi entorno piensa que soy estafador y que me estoy aprovechando de la amistad para sacar dinero, Yo me siento afectado con algo que no haría jamás en mi vida, no es ético. Perdí amigos, perdí familia, por injerencias a mi vida que no son justas.

Tercer entrevistado: Yo pienso que no hay violación a la intimidad, porque se vulnera el derecho a la intimidad cuando le han difundido material que sí es suyo y hablamos de casos como por ejemplo en México la Ley Olimpia, pero si a mí me toman mi imagen en un video que nada que ver conmigo, probablemente no está entrando en el ámbito de la intimidad sino más bien el honor, buen nombre, libre desarrollo de la personalidad.

Cuarto entrevistado: Sí, considero que se genera vulneración ya que, si su uso no es ético, es decir, si es mal utilizado por parte del usuario puede generar bullying, injerencias, odio, juicios a la persona afectada por el video, o cualquier tipo de manipulación a su imagen que haya sufrido.

Quinto entrevistado: Sí, hay una clara vulneración a sus derechos, y las consecuencias de tal manipulación pueden ser muy fuertes, afectando no solo la reputación de las personas, sino también su vida privada y relaciones familiares. Además, la capacidad de alterar y distribuir rápidamente este tipo de contenido amplifica el daño, exponiendo a las víctimas a situaciones de acoso, extorsión o chantaje.

Comentario de la autora: De acuerdo con las respuestas que se evidencian, se deduce que la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial tiene un impacto significativo en la intimidad personal y familiar, además de afectar otros aspectos de la vida de las personas. El primer entrevistado subraya que la manipulación de videos puede falsamente presentar a una persona, constituyendo una violación de la intimidad y destaca que la falta de conocimiento sobre las TIC en nuestro país agrava el problema. El segundo entrevistado describe cómo la manipulación de archivos afectó gravemente su vida

personal, llevando a la pérdida de amigos y familiares, lo cual resalta el profundo impacto emocional y social que se puede dar como consecuencia. Por otro lado, el tercer entrevistado ofrece una perspectiva diferente, argumentando que no hay violación a la intimidad si el material manipulado no pertenece realmente a la persona afectada, determina que el problema reside más en el honor, el buen nombre y el libre desarrollo de la personalidad. El cuarto entrevistado coincide con los primeros en que la manipulación de archivos sí vulnera la intimidad, especialmente cuando se usa de manera no ética y el quinto entrevistado enfatiza que se afecta la vida privada y las relaciones familiares, debido a la rápida difusión de este contenido.

En resumen, la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial vulnera a la intimidad personal afectando sus relaciones y salud mental.

Tercera pregunta:

¿Cree usted que la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial contribuye a la vulneración del derecho a la intimidad personal y familiar?

Respuestas:

Primer entrevistado: Sí, porque esta comunicación no solamente violenta la intimidad de carácter personal sino también de carácter familiar, educacional, comunitario, porque no está regulado, va desde propaganda comercial hasta pornográfica, debería regularse esto también en las instituciones.

Segundo entrevistado: Sí, porque yo pensé en demandar, pero me asesoré con un abogado el cual mencionó que el accionante debe tener un accionado, teniendo en cuenta que hay miles de hackers resulta imposible llegar al responsable. Si hubiera una ley sobre esto fuera lo ideal, porque yo cuento con pruebas de todo, pero el culpable no es posible de encontrar, y es grave pensar que si no hay un culpable presente no se considere un delito.

Tercer entrevistado: No necesariamente, salvo que, la base para ese video de Inteligencia Artificial haya sido un video que era exclusivamente almacenado en repositorios que son de uso único mío, porque recordemos que las redes sociales son públicas, el momento que

nosotros aceptamos el acuerdo de confidencialidad con las redes sociales estamos cediendo nuestra imagen a la plataforma y por ende es público y pueden verse manipulados.

Cuarto entrevistado: Sí, y esto queda abierto a la persona actora ya que antes de hacer uso de una aplicación de Inteligencia Artificial usualmente se aceptan términos y condiciones, pero pese a ello se arriesgan a su uso y deben ser consecuentes con sus actos.

Quinto entrevistado: Sí, de hecho, por esta falta de tipificación en la ley provoca que este gran daño no se considere un delito y cada vez aumente más la irresponsabilidad de aquella gente inescrupulosa que realiza este tipo de acciones.

Comentario de la autora:

Cuatro de los entrevistados responden positivamente a la pregunta establecida, estableciendo que efectivamente la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial contribuye a la vulneración del derecho a la intimidad personal y familiar. Los entrevistados coinciden en aquella necesidad de regular este problema, porque sin un marco legal claro resulta difícil identificar y responsabilizar a los culpables, agravando el daño cometido. Además, el uso de redes sociales implica una cesión de privacidad, que permite la manipulación de datos personales. Sin embargo, uno de los entrevistados. Sin embargo, uno de los entrevistados no cree que la manipulación de archivos mediante Inteligencia Artificial constituya necesariamente una violación a la intimidad, argumentando que la cesión de imagen a plataformas públicas como redes sociales implica un acuerdo de confidencialidad que podría permitir la manipulación de datos personales sin vulnerar directamente la intimidad.

Cuarta pregunta:

¿Estima usted que tipificando y sancionando en la legislación penal ecuatoriana la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial se garantiza el efectivo goce del derecho a la intimidad personal y familiar?

Respuestas:

Primer entrevistado: Sí claro, puesto que estamos en una sociedad sin ética, y ese es un gran peligro para la humanidad y mucho más cuando los medios de comunicación tergiversan el comportamiento de nuestra sociedad.

Segundo entrevistado: Obviamente, porque si apenas se pasara una situación así, de inmediato acudiría a denunciar, y con ello la afectación será mínima. Porque no hay como detener este peligroso daño, y pienso que, al haber una ley al respecto, sí pudiéramos reclamar nuestros derechos y hacerlos prevalecer.

Tercer entrevistado: Basándome en el artículo 82 de la Constitución de la República que nos habla sobre la seguridad jurídica, que nosotros tenemos el derecho a desenvolvemos dentro de un marco de normas preestablecidas. Considero que si debe haber una reforma puesto que tenemos que tener por lo menos un mínimo de normas preestablecidas que nos protejan de estas situaciones, aunque aún no tenemos una estadística para definir esto, pero de acuerdo al artículo mencionado debe haber normas que nos resguarden.

Cuarto entrevistado: Creo que sí, porque los usuarios teniendo conocimiento de una posible sanción por el daño causado, harán uso de la Inteligencia de forma responsable.

Quinto entrevistado: Sí, debería controlarse y sancionar de forma proporcional al daño causado para controlar este tipo de acciones.

Comentario de la autora: Teniendo en consideración las respuestas proporcionadas por los entrevistados, podemos inferir que existe un consenso entre todos los entrevistados sobre la necesidad imperiosa de tipificar y sancionar la manipulación de archivos mediante Inteligencia Artificial en la legislación penal ecuatoriana. Los entrevistados destacan que una regulación efectiva no solo protegería el derecho a la intimidad personal y familiar, sino que también promovería un uso más ético de la tecnología. Además, se destaca la importancia de contar con normas claras y preestablecidas que resguarden a la sociedad frente a estos riesgos emergentes, como lo respalda el marco constitucional ecuatoriano en su artículo 82 referente a la seguridad jurídica.

Quinta pregunta:

¿Qué otras soluciones sugieren usted frente al problema planteado?

Respuestas:

Primer entrevistado: Políticas de Estado, políticas de comunicación, para que haya filtros y solo ingrese información que el propio Estado la haya procesado para que sirva para la comunidad, para las personas, para la familia, no puede ingresar cualquier tipo de información,

aunque al parecer no hay interés porque los altos mandos prefieren una sociedad inconsciente para poder ejercer cierto tipo de manipulación.

Segundo entrevistado: Que dentro de la justicia ecuatoriana hubiera una tipificación, una instancia a donde acudir diciendo me realizaron tal daño, aunque no se diera con el culpable, pero que hubiera como detener mediante la eliminación de estos videos fuera suficiente.

Tercer entrevistado: Las soluciones que sugiero van más fuera del lado jurídico y se van más al lado de la comunicación social, yo creo que lamentablemente lo hacen páginas comerciales y nuestro gobierno que invierte gran cantidad recursos en marketing debería estar a la par con esto, y sin embargo por cada 100 videos de estafa tal vez 1 dice evita caer en estafas, yo pienso que tenemos una dirección de telecomunicaciones que debería de encabezar una medida que pueda permitir controlar el problema.

Cuarto entrevistado:

- Términos y condiciones claras para el uso de la Inteligencia Artificial.
- Normativa de sanción al mal uso.
- Cada sitio web o aplicación que use la Inteligencia Artificial, debería tener detector de situaciones de vulneración de tal forma que al detectarla se suspenda.

Quinto entrevistado:

- Educación para el uso de las nuevas tecnologías.
- Crear criterio para juzgar este tipo de comportamientos.
- Campañas para el buen uso de la Inteligencia Artificial.

Comentario de la autora:

Para abordar el problema planteado, se sugieren diversas soluciones por parte de los entrevistados, el primer entrevistado propone políticas estatales y de comunicación que filtren la información para proteger a la comunidad y evitar manipulaciones por parte de los altos mandos, el segundo entrevistado sugiere establecer una tipificación dentro del sistema judicial ecuatoriano para permitir denuncias y medidas de eliminación de contenido dañino, aunque no se identifique al responsable. Por su parte, el tercer entrevistado enfoca las soluciones en mejorar las prácticas de comunicación social, instando al gobierno y a las entidades relevantes a invertir más recursos en educación y campañas informativas sobre el uso responsable de la

tecnología. El cuarto entrevistado propone términos y condiciones claros para el uso de la Inteligencia Artificial, una normativa de sanciones por mal uso, y la implementación de detectores de vulneraciones en plataformas que empleen esta tecnología. Y para finalizar, el quinto entrevistado plantea soluciones como educación en tecnología, establecimiento de criterios judiciales específicos para estos casos, y campañas que promuevan el uso ético de la Inteligencia Artificial. Estas propuestas abarcan desde promover un marco regulatorio hasta iniciativas educativas y de concienciación, buscando así mitigar los efectos negativos de la manipulación de archivos mediante Inteligencia Artificial.

Sexta pregunta:

¿Qué medidas considera necesarias para concienciar a la sociedad sobre los riesgos asociados a la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial en el contexto de las nuevas tecnologías en la actualidad?

Respuestas:

Primer entrevistado: Primero que, los padres deberían tener un conocimiento sobre este tipo de comunicación, siendo deber de las instituciones de educación concientizar a las personas para que los estudiantes hagan uso de estas tecnologías en la medida de lo estrictamente necesario, porque la dominación del ser humano se da a través de la ignorancia.

Segundo entrevistado: Considero que se debe ser bastante cautos y sensatos, procurando entender bien los mensajes y la información que vemos, estos videos mediante el uso de la Inteligencia Artificial todo lo que dice lo hace un mismo tono de voz, creo que debemos aprender a descifrar los mensajes y tomarlos con cautela. Hoy los estudiantes hacen un mal uso de la Inteligencia Artificial, siendo dependientes de ello y evitando avanzar en el conocimiento, la Inteligencia es muy buena porque da la oportunidad de innovarse, pero existe mucho facilismo por su forma de generar información que se le pida de forma automática.

Tercer entrevistado: Primero, ser transparente porque la gente conoce tu solvencia. Segundo, controlar mucho lo que publicamos en redes sociales. Tercero, contrastar la información, verificar la legitimidad de las fuentes.

Cuarto entrevistado: Implementar campañas de educación y sensibilización a través de medios de comunicación, redes sociales y plataformas educativas que informen sobre los riesgos y las implicaciones éticas de la manipulación de contenido multimedia.

Quinto entrevistado:

- Que tengan un marco regulatorio el cual permita su uso, y se controle las acciones que se realizan con este tipo de tecnología.
- Proponer la idea de crear identidad digital para que la sociedad conozca el responsable de cualquier acción en el entorno digital y se minimice el anonimato.

Comentario de la autora:

Teniendo como preámbulo las respuestas de los entrevistados, se determina que es fundamental concienciar a la sociedad sobre los riesgos que se dan como consecuencia de la manipulación de archivos de video, imagen o voz mediante la utilización Inteligencia Artificial. El primer entrevistado sugiere que los padres y las instituciones educativas deben educar a los estudiantes sobre el adecuado uso de estas tecnologías. Así mismo, hay consenso sobre la necesidad de fomentar un entendimiento crítico de los contenidos y mensajes, como menciona el segundo entrevistado. Además, el tercer entrevistado enfoca la transparencia en el uso de redes sociales y la verificación de la información. El cuarto entrevistado menciona campañas de sensibilización, y el quinto entrevistado propone la implementación de un marco regulatorio como algo esencial para controlar y responsabilizar las acciones en el entorno digital, además destaca la creación de una identidad digital y considera que puede ayudar a minimizar el anonimato y asegurar que las personas sean conscientes de las implicaciones éticas de sus acciones en línea.

6.3. Estudio de casos

En la presente investigación, se analiza el estudio de casos que se encuentran relacionados con la utilización de la Inteligencia Artificial para manipular archivos de video, imagen o voz y su consecuente vulneración al derecho a la intimidad personal y familiar. Es importante mencionar que, al ser un tema relativamente nuevo, no existen sentencias ejecutoriadas, pero es preciso mencionar que basta con revisar los siguientes casos para respaldar la propuesta de reforma planteada.

6.3.1. Caso Nro. 1.

Datos referenciales:

Título: FGE alerta a la ciudadanía sobre la activación de una malintencionada campaña

Boletín de prensa: FGE N° 049-DC-2023

Fecha: 19 de septiembre de 2023

Lugar: Quito - Ecuador

Link de la noticia: <https://www.fiscalia.gob.ec/accesibilidad/fge-alerta-a-la-ciudadania-sobre-la-activacion-de-una-malintencionada-campana/>

Contenido:

La Fiscalía General del Estado alerta a la ciudadanía respecto a la activación de una malintencionada campaña que tiene como objetivo menoscabar la imagen de la fiscal general del Estado, Diana Salazar Méndez, a través del montaje de audios y videos creados utilizando inteligencia artificial.

Fiscalía ha tenido acceso a información que da cuenta de esos burdos intentos de desprestigio, con los que ciertos sectores buscan desesperada y nuevamente obtener impunidad en los casos que lleva la máxima autoridad de esta Institución. La Fiscalía General del Estado rechaza enfáticamente estas acciones, invita a la opinión pública a informarse por canales oficiales y reitera su compromiso de seguir trabajando en pro del acceso a la justicia y en contra de todo tipo de delitos. (Fiscalía General del Estado, 2023, pág. 1)

Comentario de la autora:

En la presente noticia por parte de la Fiscalía General del Estado se evidencia una alerta sobre una campaña malintencionada dirigida contra la fiscal general Diana Salazar Méndez, mediante el uso de la inteligencia artificial para crear audios y videos falsos, que pone de manifiesto las crecientes amenazas que plantea la manipulación digital. En esta situación, este tipo de ataque no solo se buscó desprestigiar a una autoridad, sino que también intentan socavar la confianza pública. Pero esta situación no solo se presenta ante personas de relevancia pública, si no que toda la ciudadanía en general está expuesta a este tipo de vulneraciones. Considero que es esencial este tipo de alertas a la ciudadanía, para que se informe acerca de este problema y siempre recurra a fuentes oficiales para obtener información verídica. Además, la

determinación de la Fiscalía de rechazar rotundamente estos actos de desinformación reafirma su compromiso con la justicia y la transparencia y es un recordatorio de la importancia de apoyar a las instituciones que trabajan en la protección del Estado de Derecho y en la persecución de delitos, incluso cuando enfrentan ataques de desinformación, aún más en esta era digital donde se evidencia una creciente manipulación informativa.

6.3.2. Caso Nro. 2

Datos referenciales:

Título: Fiscalía investiga supuesta pornografía con menores en un Colegio de Quito

Fecha: 05 de octubre de 2023

Autor: Redacción Primicias

Lugar: Quito - Ecuador

Link de la noticia: <https://www.primicias.ec/noticias/sucesos/pornografia-colegio-quito-inteligencia-artificial/>

Contenido:

La tarde del 5 de octubre de 2023, la Fiscalía informó la apertura de una investigación previa por el presunto delito de pornografía con utilización de niños, niñas y adolescentes. En este caso no hubo una denuncia previa, sino que la indagación se abrió de oficio. Esto tras la noticia de que, en una unidad educativa de Quito, se difundieron imágenes y videos de estudiantes, modificados mediante inteligencia artificial (IA) La alerta inicial la dio el grupo Rescate Escolar, el cual afirmó que se usaron técnicas de inteligencia artificial (IA) para distorsionar fotografías de más de 20 alumnas de un plantel religioso de la capital.

Tras la difusión de este caso, el Ministerio de Educación lo catalogó como violencia digital, no mencionó la posibilidad de que se trate de pornografía. La entidad recordó que ya existe un protocolo para tratar estos casos. Este documento "establece lineamientos, con el fin de garantizar la prevención, detección, intervención, derivación, seguimiento y reparación frente a situaciones de violencia digital". (Redacción Primicias / EFE, 2019, pág. 1)

Evidencia:



Fuente: Diario Primicias.

Comentario de la autora:

Según se relata en el diario Primicias, la Fiscalía anunció la apertura de una investigación preliminar por el presunto delito de pornografía infantil, relacionada con la utilización de Inteligencia Artificial. La investigación se inició de oficio, luego de que el grupo Rescate Escolar alertara sobre el suceso, se trataba de la creación y difusión de imágenes y videos manipulados con el uso de la Inteligencia Artificial en una unidad educativa de Quito. Este caso pone en evidencia las graves amenazas que plantea la manipulación digital y el uso indebido de la inteligencia artificial, no solo se afecta la intimidad y seguridad de los menores involucrados, sino que también se enfatiza la necesidad urgente de contar con un marco legal claro para la prevención y manejo de este tipo de delitos. La acción de la Fiscalía al iniciar una investigación de oficio muestra un compromiso claro con la protección de los derechos de los niños y adolescentes, pero es fundamental que la ciudadanía se mantenga informada y que se recurra a fuentes oficiales para obtener información verídica, y sobre todo se informe de los riesgos relacionados al uso indebido de la Inteligencia Artificial. Es de suma importancia destacar que este proceso no se encuentra públicamente visible debido a la reserva legal por minoría de edad.

6.3.3. Caso Nro. 3.

Datos referenciales:

Título: Imágenes o audios manipulados con inteligencia artificial de los presentadores de Televistazo circulan en redes

Fecha: 09 de julio de 2024

Autor: Periodista digital de Ecuavisa

Lugar: Quito - Ecuador

Link de la noticia: <https://www.ecuavisa.com/noticias/seguridad/imagenes-o-audios-manipulados-con-inteligencia-artificial-de-los-presentadores-de-televistazo-circulan-en-redes-YB7641320>

Contenido:

La imagen de presentadores de Televistazo es usada de manera fraudulenta en redes sociales para estafar a la ciudadanía mediante una manipulación de imágenes con inteligencia artificial. También se direcciona a las víctimas a un portal web falso clonando el de Ecuavisa. El deepfake es un video, imagen o audio manipulado con inteligencia artificial que imita la apariencia y voz de una persona aparentando que está haciendo o diciendo cosas que en la realidad no ocurrieron. Esta técnica, que se ha convertido en una tendencia en internet, también se usa para actos ilícitos. En redes sociales como Facebook e Instagram están circulando Deepfakes en los que se utiliza la imagen de presentadores de Televistazo y el logo de Ecuavisa para hacer anuncios falsos, intentando estafar a los usuarios. En los videos se ofrecen fraudulentas formas de ganar dinero rápido, como supuestos influencers.

Comentario de la autora:

En esta noticia por parte de la cadena de televisión Ecuavisa, se narra cómo la imagen de los presentadores de Televistazo está siendo utilizada de manera fraudulenta en redes sociales para estafar a la ciudadanía mediante la manipulación de imágenes con inteligencia artificial. La manipulación de imágenes y videos con inteligencia artificial, como es el caso de los Deepfakes, representa una amenaza significativa para la intimidad personal y familiar, la integridad de la información y la seguridad de los ciudadanos. Este incidente, en el que se utilizan las imágenes de los presentadores de Televistazo para crear contenido falso, no solo busca engañar y estafar a las personas, sino que también socava la confianza en los medios de comunicación y las plataformas digitales, por ello es indispensable que la ciudadanía esté alerta y se informe sobre las técnicas utilizadas por los estafadores para no caer en estos engaños. La educación y la concientización sobre los Deepfakes y otras formas de manipulación digital son esenciales para protegerse de fraudes y desinformación.

7. Discusión

7.1. Verificación de objetivos

Para la elaboración del presente Trabajo de Integración Curricular se estableció un objetivo general, tres objetivos específicos, que se detallan y verifican a continuación.

7.1.1. Objetivo general

El objetivo general propuesto es **“Realizar un estudio, doctrinario y jurídico sobre la manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial y su vulneración al derecho a la intimidad personal y familiar”**.

El objetivo general de este estudio ha sido debidamente verificado a lo largo del desarrollo del marco teórico, puesto que, se llevó a cabo un análisis exhaustivo y puntualizado del tema, apoyándose en fuentes doctrinales y en la legislación vigente. Mediante el uso de la doctrina y la ley, se abordaron y desarrollaron todos los aspectos concernientes a este objetivo y se ha comprobado que la manipulación de archivos de video, imagen o voz mediante herramientas de Inteligencia Artificial causa una vulneración al derecho a la intimidad personal y familiar. Los temas que es pertinente destacar son, la Terminología jurídica, especialmente el término Deepfakes, la Inteligencia Artificial, El Derecho a la Intimidad personal y familiar.

Además, se destacó la necesidad de un marco regulatorio para proteger los derechos fundamentales en el contexto de la creciente adopción de tecnologías de Inteligencia Artificial.

En este ámbito se ha podido comprender cada parte del proceso de manipulación de estos archivos, considerando no solamente la legislación nacional sino que también se puntualizó lo que las legislaciones de otros países nos establecen al respecto, pudiendo comprender de esta manera que este campo de la informática como lo es la Inteligencia Artificial se debe manejar con mucha ética, y es necesario que el Estado como ente regulador de derechos, establezca limitaciones en nuestro país, aunque no sean casos mayoritarios, es algo que está avanzando a pasos agigantados y se debe tener la plena certeza que la ciudadanía cuenta con seguridad jurídica y no se vea en la terrible situación de no poder acudir ante la ley porque no hay una ley que tipifique este delito.

El análisis que se pudo evidenciar, ha permitido conocer todo lo relacionado al Derecho Informático y a procesos de criminalización, judicialización y penalización, además de

entender a fondo el delito y todos sus elementos. Todos los temas y subtemas que contiene el marco teórico, se ajustan a la problemática planteada, brindando con ello, un estudio absoluto de todo lo que ayuda a la manipulación de archivos de video, imagen o voz para perjudicar la garantía del derecho a la intimidad tanto personal como familiar. Fundamentación jurídica de la propuesta de reforma legal

En lo que concierne al estudio jurídico se lo realizó a través de un análisis e interpretación determinante de las normas jurídicas que se encuentran relacionadas con la vulneración de derechos fundamentales, especialmente el derecho a la intimidad personal y familiar, mismos que están reconocidos plenamente por la Constitución de la República del Ecuador y que son vulnerados por esta causa. Para ello se tuvo en cuenta la Constitución de la República del Ecuador, el Código Orgánico Integral Penal, y la Ley de Comercio Electrónico, Firmas y Mensajes de Datos; como normativa nacional pertinente, y, como normativa extranjera se tomó en consideración Europa, España y México, con el Reglamento de la Unión Europea, Código Penal de España, y el Código Penal del Estado de Sinaloa, respectivamente.

Al examinar la legislación nacional e internacional, se busca identificar las mejores prácticas y los principios fundamentales que deben guiar la regulación del uso de herramientas de inteligencia artificial para la manipulación de archivos de video, imagen o voz. Se evalúan aspectos clave como el respeto a la intimidad en todos sus ámbitos, la legalidad de dichas prácticas, la garantía de protección de los derechos individuales y la prevención del abuso tecnológico.

7.1.2. Objetivos específicos

- 1. “Establecer las afectaciones al derecho a la intimidad personal y familiar por la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial.”**

Este objetivo específico se pudo verificar acorde a lo establecido en la primera pregunta de la encuesta: Estima usted que con la manipulación de archivos de video, imagen o voz mediante la Inteligencia Artificial se afecta principalmente: **El derecho a la intimidad personal y familiar, el derecho al honor y buen nombre, el derecho a la protección de datos de carácter personal, el derecho a la verdad.**

Debido a que, por el planteamiento de esta pregunta se verifica que la mayoría de los encuestados, respondieron que el principal derecho afectado es el derecho a la intimidad personal y familiar, sin embargo, la minoría respondió que efectivamente las afectaciones se dan al derecho al honor y buen nombre, a la protección de datos de carácter personal y el derecho a la verdad. Un aspecto que se destaca de este resultado es que el los encuestados consideran que la manipulación de archivos de video, imagen o voz mediante la Inteligencia Artificial, no se encuentra limitado solamente a la vulneración del derecho a la intimidad personal y familiar, si no que se considera como una circunstancia que produce una pluralidad de consecuencias. Siendo así que, es fundamental tomar acciones prontas para salvaguardar estos derechos y proteger a la sociedad de estos ataques tecnológicos, en el auge de la Inteligencia Artificial; Por su parte, este objetivo también se verifica con la primera pregunta de la entrevista, en donde los entrevistados determinaron que la afectación principal es al derecho a la intimidad personal y familiar, pero destacan la existencia de algunas otras afectaciones como la privacidad de las víctimas, la vulneración al derecho al honor y buen nombre y su consecuente daño a la reputación del individuo, en base a ello, se puede manifestar la vulneración es evidente y las afectaciones son múltiples, en todos los aspectos de la vida de la persona afectada, en el ámbito individual pero también a su entorno; A su vez, el objetivo se verifica con el derecho comparado, puesto que, el Reglamento a la Inteligencia Artificial establece un marco legal ético sobre el uso de esta tecnología, intentando garantizar que no existan afectaciones de ningún tipo hacia la ciudadanía, siempre y cuando el uso sea responsable y acorde a lo estrictamente establecido, el Código Penal de Sinaloa determina de igual forma, la afectación de la Inteligencia Artificial hacia la intimidad sexual, garantizando la protección debida a la generación de este contenido falso en el índole sexual, que sus consecuencias son bastante severas, como daño psicológico, bullying y demás cuestiones que pueden suscitarse debido a este problema, el enfoque comparativo entre estas legislaciones permitió identificar las fortalezas y debilidades del marco legal existente en Ecuador en relación con los modelos de otros países. Además, establece las bases para proponer reformas legislativas y políticas que contribuyan a proteger la intimidad personal y familiar, y a promover un uso ético y responsable de las tecnologías de inteligencia artificial.; De igual manera con el análisis de las noticias, en el segundo caso se evidencia que dos alumnos de un colegio de Quito manipularon fotos de más de 20 alumnas de la misma institución, utilizando la Inteligencia Artificial, con el objetivo de generar videos pornográficos falsos sobre ellas, causando una afectación realmente violenta sobre las víctimas, dañando su honor y buen

nombre, su seguridad, y una situación de violencia digital grave, sobre todo en este caso que las víctimas son menores de edad.

2. Demostrar la vulneración a la intimidad personal y familiar por la manipulación de archivos de video, imagen o voz mediante el uso de la inteligencia artificial.

El segundo objetivo específico se logra verificar mediante la aplicación de encuestas, concretamente en el planteamiento de la segunda pregunta que determina: **¿Cree usted que con el uso de la Inteligencia Artificial en la manipulación archivos de video, imagen o voz se viene afectando gravemente el derecho a la intimidad personal y familiar?**, y en base a los resultados obtenidos la mayoría de los encuestados respondieron acertadamente a este pregunta, destacando que esta tecnología afecta gravemente al derecho a la intimidad personal y familiar, pues la regulación de este problema en nuestro país es ineficiente. De igual forma, en la segunda y tercera pregunta de la entrevista se constata que efectivamente existe una clara vulneración al derecho mencionado, destacando que esta situación afecta la vida privada y entorno de la víctima, siendo así que el daño ocasionado es de gravedad. Asimismo, en el estudio de casos se observa una clara vulneración a este derecho constitucional, siendo así que en el primer caso observamos una afectación directa hacia la Fiscal General del Estado perjudicando su imagen con videos y audios manipulados usando la Inteligencia Artificial, agrediendo si vida privada ante injerencias no consentidas sobre actos ficticios. De esta forma podemos evidenciar que, en las encuestas, entrevistas y estudio de casos, se verificó el cumplimiento del segundo objetivo específico planteado en esta investigación.

3. Presentar un proyecto de reforma legal al régimen penal ecuatoriano, tipificando y sancionando la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial para garantizar el derecho a la intimidad personal y familiar.

Este tercer y último objetivo específico se logró verificar por medio de los resultados obtenidos a través de las encuestas y las entrevistas propuestas como técnicas de campo, particularmente en la cuarta pregunta de la encuesta, que establece que: **¿Está usted de acuerdo en tipificar y sancionar en la legislación penal ecuatoriana la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial para garantizar el derecho a la intimidad personal y familiar?**, donde se constató que la mayoría, está de acuerdo con esta tipificación y sanción en el Código Orgánico Integral Penal, enfatizando que la penalización

de este problema es necesaria, puesto que el derecho no debería ir detrás de los avances tecnológicos, porque de ser así, se vulnerará derechos fundamentales y sobre todo la seguridad jurídica de las personas como sujetos de derechos. Por su parte, también se verifica en la cuarta pregunta de la entrevista, que los entrevistados mayoritariamente aceptaron que es necesaria una reforma legal para que se respete la seguridad jurídica, pues todos los ciudadanos tenemos derecho a vivir dentro de un marco de normas preestablecidas, en este caso, para que se garantice el derecho a la intimidad personal y familiar dentro del ámbito tecnológico; Es determinante destacar que también se logra verificar este objetivo mediante el análisis de las noticias planteadas en el estudio de casos, por ejemplo en el tercer caso el canal de televisión abierta Ecuavisa declaró que se han estado usando herramientas de Inteligencia Artificial para manipular imágenes o audios de algunos de sus presentadores, estas manipulaciones se encuentran en las redes sociales con el fin de estafar a la ciudadanía mediante anuncios falsos, es por ello la importancia de su regulación, ya que esta situación se encuentra en auge en nuestro país, y se han determinado casos desde vulneración a menores, anuncios fraudulentos, hasta desprestigio de autoridades, y muchos más, que son motivo suficiente para que exista una tipificación y sanción como delito dentro de nuestro Código Orgánico Integral Penal.

Finalmente, el derecho comparado resulta de vital importancia para la verificación del presente objetivo, específicamente el Código Penal de Sinaloa tipifica y sanciona la utilización de la Inteligencia Artificial para manipular archivos de video, imagen o voz, y atentar contra la intimidad sexual de los individuos. Además, claramente determina lo que se entenderá como Inteligencia Artificial para atender a la importancia del tenor literal de la ley. Lo cual resulta significativo para poder establecer un marco legal claro dentro de nuestra legislación, tomando el ejemplo del derecho comparado, para preservar la justicia y el bien común.

7.2. Hipótesis

La hipótesis propuesta para la presente investigación es **“La falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”**.

La hipótesis planteada se comprueba a través de los resultados obtenidos en las encuestas y entrevistas realizadas que destacan la necesidad urgente de una reforma al Código Orgánico Integral Penal. Dichos resultados resaltan que, de no abordarse esta problemática con prontitud,

podría aumentar de manera incontrolable, resultando en la vulneración de los derechos de un número considerable de ciudadanos.

Concretamente, las entrevistas revelan una creciente preocupación entre los profesionales del derecho y especialistas en informática sobre la capacidad actual del marco legal para abordar los desafíos que presenta la inteligencia artificial en la manipulación de archivos de video, imagen y voz. Por su parte, las encuestas reflejan un consenso sobre la necesidad de fortalecer las regulaciones y establecer medidas preventivas para proteger la intimidad personal y familiar. Además, los datos sugieren que, sin una intervención legislativa adecuada, el uso indebido de estas tecnologías podría tener consecuencias graves y difíciles de revertir, afectando la confianza pública en el sistema legal y la percepción de seguridad jurídica. Por lo tanto, se recomienda una revisión integral del Código Orgánico Integral Penal y la implementación de políticas específicas que aborden estos nuevos retos tecnológicos, asegurando así la protección efectiva de los derechos constitucionales de los ciudadanos.

Esta hipótesis también se verifica de acuerdo con lo establecido en el estudio de casos, pues en nuestro país ha sido de conocimiento público que existen videos manipulados con herramientas de Inteligencia Artificial que han socavado la confianza pública, pues son videos ficticios sobre personas reales, creando una falsa representación sobre su persona, que desmeritan, desprestigian y vulneran sus derechos, principalmente el derecho a la intimidad personal y familiar. Y en las legislaciones tanto de la Unión Europea como del Estado de Sinaloa, se determina abiertamente que el uso malintencionado de la Inteligencia Artificial para crear videos falsos sobre un individuo, haciendo énfasis que esta tecnología lo realiza con un nivel impresionante de realismo que es difícil distinguir si es real o no, vulnera la intimidad en todos sus ámbitos.

7.3. Fundamentación jurídica para la propuesta de Reforma Legal.

La iniciativa de una reforma legal se fundamenta en la ausencia de regulación en la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial. Este problema vulnera gravemente el derecho a la intimidad personal y familiar, creando una situación problemática debido al uso indebido de estas herramientas tecnológicas. La manipulación de estos archivos puede llevar a la difusión de información falsa, el chantaje, la difamación, la estafa, la discriminación y otras formas de abuso que afectan no solo a individuos en el ámbito personal, sino también en el ámbito familiar. La falta de un marco

legal adecuado para enfrentar estos problemas deja a las víctimas sin protección y a los infractores sin una sanción, dando como resultado que las personas que cometen este tipo de actos, queden impunes.

En este contexto, el modelo jurídico del Estado de Sinaloa, perteneciente a México, en su Código Penal ya contempla penas para quienes difundieran contenido íntimo sin consentimiento, y amplía esta protección al incluir la manipulación de estos contenidos mediante Inteligencia Artificial, reflejando un enfoque proactivo para enfrentar las nuevas formas de violación de la intimidad. Además, considero que este enfoque es innovador, ya que otorga la debida importancia a penalizar el uso indebido de estas herramientas tecnológicas, y es importante resaltar que dentro de esta normativa se encuentra especificado claramente lo que se entiende por Inteligencia Artificial. Aunque la regulación establecida en el Código Penal de Sinaloa se centra en la intimidad sexual, es primordial reconocer que nuestra Constitución garantiza el efectivo goce del derecho a la intimidad personal y familiar, y según ello, la reforma legal propuesta busca fortalecer esta protección según los principios constitucionales.

La reforma legal busca asegurar una protección integral del derecho a la intimidad, adaptándose a la realidad tecnológica actual y subrayando la importancia de mantener la privacidad frente a las amenazas emergentes. Esta actualización legislativa es crucial para garantizar que el marco jurídico se mantenga alineado con los avances digitales, proporcionando una protección robusta contra las nuevas formas de abuso tecnológico.

La base legal de la propuesta de reforma se enfoca en salvaguardar el derecho constitucional a la intimidad personal y familiar, el cual otorga a las personas el control sobre su círculo íntimo y la protección contra la divulgación no deseada de información personal. Sin embargo, los avances tecnológicos, en particular en el ámbito de la Inteligencia Artificial, han dado lugar a nuevas formas de manipulación de contenidos que amenazan este derecho fundamental, teniendo en consideración que esta habilidad para crear videos, imágenes y audios falsificados con un alto grado de realismo, representa un riesgo considerable para la integridad psicológica y la reputación de las víctimas. Además, también se debe destacar la rápida evolución de la tecnología, y el papel del sistema penal en estos casos, pues el derecho, debería evolucionar en línea con el ámbito digital, para así poder garantizar una protección efectiva de los derechos.

Por lo tanto, es fundamental que la legislación ecuatoriana se actualice en estos temas, el Código Orgánico Integral Penal necesita ser actualizado para incluir disposiciones específicas

que regulen el uso de tecnologías digitales en relación con la Inteligencia Artificial para abordar estas nuevas formas de violación de la intimidad, y con ello, se pueda garantizar la protección de los ciudadanos en una sociedad cada vez inmersa en la tecnología, asegurando que el derecho a la intimidad personal y familiar se mantenga protegido frente a estas amenazas.

8. Conclusiones

Después de haber desarrollado el marco teórico y analizado los resultados de las técnicas de acopio empírico, tales como entrevistas y encuestas, y otros elementos que han sido fundamentales para este trabajo de integración curricular, se han considerado las siguientes conclusiones:

Primera: En base al estudio del derecho comparado, se ha determinado que la regulación de la Inteligencia Artificial y su uso ético ya se está dando en la Unión Europea, con su Reglamento a la Inteligencia Artificial, siendo estos países en donde existe un gran avance tecnológico, sin embargo, los países en vías de desarrollo deben tomar este ejemplo y prepararse para esta situación, como México, que en el Estado de Sinaloa ya se ha tipificado y sancionado este delito en su Código Penal de Sinaloa, y los demás países latinoamericanos están avanzando con propuestas de ley para afrontar este problema.

Segunda: De los resultados obtenidos mediante encuestas y entrevistas, se destaca que la vulneración del derecho a la intimidad personal y familiar mediante herramientas que usan Inteligencia Artificial para manipular, videos, imágenes y voces, es un problema grave. Según los encuestados y entrevistados, es necesario tipificar y sancionar este problema en nuestro Código Orgánico Integral Penal para proteger los derechos, especialmente el derecho a la intimidad personal y familiar el cual está reconocido constitucionalmente.

Tercera: Todos los objetivos propuestos se verificaron correctamente, es por ello que, a través del desarrollo de la presente investigación, se logró concluir que la manipulación de los archivos de video, imagen o voz utilizando Inteligencia Artificial, es una problemática en rápido crecimiento, y requiere que su regulación sea inmediata, este trabajo ha demostrado la gravedad del asunto y la imperiosa necesidad de tipificar y sancionarlo. Mediante una adecuada regulación, concientización y educación, es posible mitigar los impactos negativos de esta tecnología y consolidar un auténtico Estado de Derecho.

Cuarta: La hipótesis planteada se ha verificado a lo largo de este Trabajo de Integración Curricular, en base a los fundamentos teóricos y las técnicas de acopio empírico, siendo así, que se evidenció una urgente necesidad de reformar el Código Orgánico Integral Penal, porque, sin una adecuada intervención legislativa, el uso indebido de la tecnología seguirá en crecimiento, afectando gravemente a los derechos fundamentales y transgrediendo la seguridad jurídica de los ciudadanos.

Sexta: En nuestro país, no existe una regulación que especifique la manipulación digital de archivos mediante Inteligencia Artificial, lo que representa una falta de seguridad jurídica, hablando específicamente de los Deepfakes, este es un problema creciente en Ecuador y requiere atención inmediata, siendo esencial que las personas se eduquen sobre las consecuencias de esta tecnología, y le den la importancia debida para proteger su intimidad.

Séptima: Con el estudio de casos se evidenció que en Ecuador la manipulación de archivos mediante inteligencia artificial representa una amenaza grave para la intimidad de los ciudadanos. Los incidentes analizados subrayan la urgencia de implementar una regulación efectiva para prevenir y sancionar estos abusos, no solo las personas de relevancia social son afectadas, sino que toda la población, especialmente grupos vulnerables están expuestos a estos ataques a la intimidad. La manipulación de archivos multimedia mediante la Inteligencia Artificial vulnera gravemente la intimidad personal y familiar, generando un riesgo significativo para la sociedad en general, por tal motivo, se requiere una reforma legal, para garantizar el uso ético y responsable de la tecnología, protegiendo los derechos de la sociedad ecuatoriana. Mediante una adecuada regulación, concientización y educación, es posible mitigar los impactos negativos de esta tecnología y consolidar un auténtico Estado de Derecho.

9. Recomendaciones

A partir de las conclusiones alcanzadas, se sugiere adoptar las siguientes recomendaciones para abordar el problema que se ha detallado a lo largo del presente trabajo de integración curricular:

Primera: Al Estado ecuatoriano, se recomienda adoptar el modelo que nos proporciona las legislaciones de la Unión Europea y México, en relación a la Inteligencia Artificial, estableciendo claridad respecto a este tema dentro de nuestro marco legal, para con ello, mitigar el abuso tecnológico en nuestro país.

Segunda: A la Fiscalía General del Estado, la implementación de un enfoque especializado en la investigación de delitos cibernéticos relacionados con la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial, estableciendo procedimientos específicos para detectar y sancionar estos abusos. Se recomienda incluir, la formación especializada del personal en estos temas, aseguramiento de la confidencialidad de las víctimas proporcionándoles un apoyo psicológico durante el proceso judicial y colaborar estrechamente con organizaciones especializadas en el ámbito digital.

Tercera: Al Ministerio de Educación, incorporar en los programas educativos, contenidos que sensibilicen y concienticen sobre las consecuencias asociadas a la Inteligencia Artificial, Además, debe promoverse la capacitación de los docentes y estudiantes para identificar y manejar adecuadamente los problemas derivados de esta tecnología.

Cuarta: A las instituciones educativas, como las universidades, fomentar investigaciones más profundas sobre la manipulación de videos, imágenes o voz, y las implicaciones legales que derivan de la mal utilización de esta tecnología. Esto contribuirá a una mayor comprensión académica y facilitará la elaboración de propuestas legislativas y políticas públicas que respondan adecuadamente a esta problemática.

Quinta: A los medios de comunicación, verificar la autenticidad de la información antes de su publicación, desarrollando protocolos para identificar el uso de herramientas de inteligencia artificial que puedan alterar los contenidos, y con ello, perjudicar a las personas que han sido víctimas de estas manipulaciones. Esto garantizará que la información divulgada sea precisa y confiable, promoverá la transparencia, protegerá la integridad informativa y evitará la propagación de desinformación.

Sexta: Al Ministerio de Telecomunicaciones y de la Sociedad de la Información, desarrollar campañas educativas y de concientización sobre los Deepfakes como parte del uso indebido de la Inteligencia Artificial, promoviendo la creación de normativas para asegurar la protección a la intimidad personal y familiar en el entorno digital.

Séptima: A la Asamblea Nacional, que acoja el siguiente proyecto de ley para reformar el Código Orgánico Integral Penal, incorporando disposiciones específicas para tipificar y sancionar este problema, protegiendo así a todos los ciudadanos ecuatorianos, y sobre todo a los grupos más vulnerables que son más propensos a estos daños.

9.1. Propuesta de Reforma al Código Orgánico Integral Penal



LA ASAMBLEA NACIONAL DEL ECUADOR

CONSIDERANDO:

Que, el artículo 1 de la Constitución de la República del Ecuador declara que el Ecuador es un Estado constitucional de derechos y justicia siendo fundamental el respeto a esta garantía;

Que, el artículo 16 de la Constitución de la República del Ecuador reconoce el derecho de todos los ciudadanos al acceso universal a las tecnologías de información y comunicación, así como a la creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de frecuencias del espectro radioeléctrico y a bandas libres para la explotación de redes inalámbricas;

Que, nuestra Carta Magna en su artículo 17 numeral 2 dispone que el Estado se encargará de fomentar la pluralidad y diversidad en la comunicación, y, además, facilitará el acceso universal a las tecnologías de la información y comunicación en especial para las personas y colectividades quearezcan d dicho acceso o lo tengan de forma limitada;

Que, el artículo 66 numeral 19 de la Constitución de la República del Ecuador reconoce y garantiza a las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección;

Que, el artículo 66 numeral 20 de la Constitución de la República del Ecuador reconocerá y garantizará a todas las personas el derecho a la intimidad personal y familiar.

Que, el artículo 82 de la Constitución de la República del Ecuador reconoce que el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

Que, el artículo 178 del Código Orgánico Integral Penal establece que 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.

Que, el artículo 22 de la Ley de Comunicación establece que todas las personas tienen derecho a que la información de relevancia pública que reciben a través de los medios de comunicación sea verificada, contrastada, precisa y contextualizada.

En uso de la atribución que le confiere el número 6 del artículo 120 de la Constitución de la República, expide lo siguiente:

LEY REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL

Artículo uno.- Al final del Art. 178 agréguese un inciso con el siguiente texto:

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.

Será sancionada con pena privativa de libertad de tres a cinco años, la persona que, utilizando Inteligencia Artificial, manipule archivos de video, imagen o voz, sin el consentimiento de la persona afectada. Para los efectos de esta ley, se entenderá por Inteligencia Artificial cualquier sistema, aplicación, programa o tecnología que, mediante técnicas automatizadas, genere modificaciones de fotos, audios o videos.

DISPOSICIÓN FINAL.

ÚNICA.- La presente reforma entrará en vigor a partir de la fecha de su publicación en el Registro Oficial.

Dado en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha, a los treinta y un días del mes de julio del año dos mil veinticuatro.

MSC. HENRY FABIAN KRONFLE KOZHAYA
Presidente de la Asamblea Nacional

ABG. ALEJANDRO MUÑOZ HIDALGO
Secretario General

10. Bibliografía

- Albán Gómez, E. (2018). *Manual del Derecho Penal. Parte General*. Quito, Ecuador: EDLE S.A.
- Aliaga, G. L. (2021). Introducción práctica a la edición de vídeo con Adobe Premiere CC 2020. Universidad Miguel Hernández.
- Asamblea Constituyente. (2002). *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*. <https://doi.org/Ley N° 2002-67>
- Asamblea Constituyente. (2008). *Constitución de la República del Ecuador*. <https://doi.org/Montecristi>
- Asamblea constituyente. (2013). *Ley Orgánica de Comunicación*. <https://doi.org/REGISTRO OFICIAL - SUPLEMENTO: N° 22, Quito, 21 de junio de 2013>.
- Asamblea Constituyente, COIP. (2014). *Código Orgánico Integral Penal*. <https://doi.org/Registro Oficial - Suplemento: Año I - N.° 180>
- Asamblea General de las Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*. <https://doi.org/DUDH>
- Avogadro, M. (2009). Comunicación, redes sociales y ciberdelitos. *Razón y Palabra*, 12.
- Avogadro, M. (2012). REINVENTANDO LAS PALABRAS EN EL CIBERESPACIO: DE LA ARROBA AL SMARTPHONE INFORMACIONES DE MILLONES POR MILLÓN. *RAZÓN Y PALABRA, Prmera Revista Electrónica en América Latina Especializada en Comunicación*, 1.
- Barrera, L. (julio-diciembre de 2012). FUNDAMENTOS HISTÓRICOS Y FILOSÓFICOS DE LA INTELIGENCIA ARTIFICIAL. *Revista de Investigación y Cultura*, 1(1), 87-92.
- Becerril, D. (2014). LA EVALUACION DE LA PENALIZACIÓN AL DELINCUENTE. *Revista Internacional de Doctrina y Jurisprudencia*.
- Biblioteca del Congreso Nacional de Chile. (2024). *La Sociedad, el Derecho y el Pensamiento Político*. Obtenido de https://www.bcn.cl/formacioncivica/detalle_guia?h=10221.3/45670

- Biurrun, A. (16 de Octubre de 2021). *LA RAZÓN*. Obtenido de Deep Voice: tecnología que falsifica la voz y con la que han robado 35 millones de dólares:
<https://www.larazon.es/tecnologia/20211016/ivt7yazbmzb7lmxknhf2hz2fma.html>
- Bonilla, C., Machado, M., & Tixi, D. (2021). El juicio de tipicidad y su importancia jurídica en sentencias de carácter penal en el Ecuador. *Revista Dilemas Contemporáneos, Educación, Política y Valores*.
<https://doi.org/https://doi.org/10.46377/dilemas.v9i.3005>
- Bustos, J. (2004). *Antijuricidad y causas de justificación*. Medellín. Obtenido de
<file:///C:/Users/Usuario/Downloads/Dialnet-AntijuricidadYCausasDeJustificacion-6263236.pdf>
- Cabanellas, G. (2006). *Diccionario Jurídico Elemental*. Buenos Aires: Heliasta.
- Cambridge English-Spanish Dictionary. (03 de 07 de 2024). *Cambridge Dictionary*, online. (C. U. Press, Editor) Recuperado el 03 de 07 de 2024, de
<https://dictionary.cambridge.org/es/diccionario/ingles-espanol/deep-learning?q=Deep+learning>
- Cervigón, A. (2011). *Seguridad Informática*. PARAINFO.
- Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. (2020). *Estrategias eficaces relativas a la utilización de la tecnología, en particular la tecnología de la información y las comunicaciones, para prevenir e investigar el tráfico ilícito de migrantes*.
https://www.unodc.org/documents/treaties/WG_SOM/Website/CTOC_COP_WG.7_2_020_3/CTOC_COP_WG.7_2020_3_S.pdf: Naciones Unidas.
- Constitución Española. (1978). España: Boletín Oficial del Estado.
- Corte Interamericana de los Derechos Humanos. (2023). *Diccionario de la Corte Interamericana de los Derechos Humanos*. Obtenido de
<https://biblioteca.corteidh.or.cr/termino/48>

- Da Silva, D., Web Content, & SEO Associate. (12 de agosto de 2021). *¿Qué es el Deep Learning?* Obtenido de Blog de Zendesk: <https://www.zendesk.com.mx/blog/que-es-el-deep-learning/>
- Diccionario panhispánico del español jurídico. (2023). *Diccionario panhispánico del español jurídico*. Obtenido de <https://dpej.rae.es/lema/criminalizar>
- Elkfury, F. &. (2021). *Clasificación y representación de emociones en el discurso hablado en español empleando Deep Learning*. (v. i. RISTI-Revista Ibérica de Sistemas e Tecnologías de Información, Productor)
- Equipo editorial, Etecé. (19 de Noviembre de 2023). *Redes sociales*. Obtenido de Concepto: <https://concepto.de/redes-sociales/>.
- Ferrer, E., Martínez, F., & Figueroa, G. (2014). *Diccionario de Derecho Procesal Constitucional y Convencional*. México, D. F.: INSTITUTO DE INVESTIGACIONES JURÍDICAS.
- Franganillo, J. (2023). La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos. *methaodos.revista de ciencias sociales*, 11(2).
<https://doi.org/https://doi.org/10.17502/mrcs.v11i2.710>
- Fiscalía General del Estado. (2023). *FGE alerta a la ciudadanía sobre la activación de una malintencionada campaña*. Quito: FISCALÍA GENERAL DEL ESTADO.
- Gicovate, M. (1982). *Los procesos de decriminalización*. Caracas: Universidad Central de Venezuela, Facultad de Ciencias Jurídicas y Políticas.
- González, K. A. (13 de julio de 2024). Inteligencia artificial: ¿es urgente regularla en Ecuador? *expreso*. Obtenido de <https://www.expreso.ec/ciencia-y-tecnologia/inteligencia-artificial-urgente-regularla-ecuador-206524.html>
- Granero, M. (17 de marzo de 2023). *D-ID: plataforma de creación de videos con inteligencia artificial*. Obtenido de Yeswelab: <https://yeswelab.com/blogs/aplicaciones-de-la-inteligencia-artificial/plataforma-creacion-videos-inteligencia-artificial-d-id>

- Gutiérrez, A. y. (14 de julio de 2020). Inteligencia Artificial (IA) Aplicada en el. *Revista Derecho y Realidad*, 53-80.
<https://doi.org/https://doi.org/10.19053/16923936.v18.n35.2020.9638>
- Honorable Congreso del Estado de Sinaloa. (1992). *Código Penal del Estado de Sinaloa*.
<https://doi.org/Publicado en el Periódico Oficial, No. 131>
- Künsemüller, C. (2005). La judicialización de la ejecución penal. *Revista de Derecho (Valparaiso)*, 1(XXVI).
<https://doi.org/https://www.redalyc.org/pdf/1736/173619921006.pdf>
- Luna, N. (24 de noviembre de 2017). Prometea: una inteligencia artificial para ayudar a la Justicia porteña. *LA NACION*.
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (diciembre de 2021). *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. Obtenido de IA en Ecuador – Documento final:
<https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2022/11/Proyecto-diagnostico-inteligencia-artificial-IA-en-Ecuador-Documento-final-JC-JO-MS-002.pdf>
- Montiel, M. (2000). Los cibermedios como nuevas estructuras de comunicación social. *Opción: Revista de Ciencias Humanas y Sociales*, 48.
- Naciones Unidas : Oficina de las Naciones Unidas Contra la Droga y el Delito En México. (23 de enero de 2023). *Naciones Unidas*. Obtenido de Inteligencia artificial para detectar y prevenir la violencia contra las mujeres:
<https://www.unodc.org/lpomex/es/noticias/enero-2023/inteligencia-artificial-para-detectar-y-prevenir-la-violencia-contra-las-mujeres.html>
- Nieto, M. M. (octubre de 2016). *Redes sociales y derecho a la intimidad de los menores de edad [en línea]*. Obtenido de Biblioteca digital de la Universidad Católica Argentina:
<https://repositorio.uca.edu.ar/handle/123456789/3048>
- ONU. (7 de septiembre de 2023). *Un niño debe tener al menos 13 años para empezar a utilizar la inteligencia artificial en las aulas*. Obtenido de Noticias ONU.

- Orellana, J. (01 de 07 de 2024). *¿Qué es machine learning y por qué es tan popular?* (Universidad de Cuenca) Recuperado el 20 de junio de 2024, de <https://www2.ucuenca.edu.ec/254-espanol/investigacion/blog-de-ciencia/ano-2019/julio-2019/1222-machine-learning>
- Ossorio, M. (2008). *Diccionario de Ciencias Jurídicas Políticas y Sociales*. Datascan, S.A.
- Parlamento Europeo. (2024). *Reglamento de Inteligencia Artificial*. Obtenido de file:///C:/Users/Usuario/Desktop/Eve/octavo%20a/TIC/LEYES%20EXTRANJERAS%20-%20DERECHO%20COMPARADO/TA-9-2024-0138_ES.pdf
- Payne , L. (16 de Abril de 2024). *Britannica*. Obtenido de <https://www.britannica.com/technology/deepfake>
- Plascencia, R. (2004). *Teoría del delito*. México, D.F: UNAM, Instituto de Investigaciones Jurídicas.
- RAE. (10 de 04 de 2024). *Diccionario de la lengua española*. Obtenido de REAL ACADEMIA ESPAÑOLA: <https://dle.rae.es>
- Real Academia Española. (2001). *Diccionario de lengua española*. Obtenido de <https://www.rae.es/drae2001/inform%C3%A1tica>
- Redacción Primicias / EFE. (3 de septiembre de 2019). La inteligencia artificial de una app en China genera preocupación sobre privacidad. *PRIMICIAS*. Obtenido de <https://www.primicias.ec/noticias/tecnologia/inteligencia-artificial-app-china-genera-preocupacion-sobre-privacidad/>
- Rouhiainen, L. (2018). *Inteligencia artificial 101 cosas que debes saber hoy sobre nuestro futuro*. Barcelona: Editorial Planeta, S.A.
- Roxin, C. (1997). *Derecho Penal Parte General - Tomo I - Fundamentos la estructura de la teoría del delito*. Madrid, España: Civitas, S. A.
- Roxin, C., Arxt, G., Gómez, L., Tiedemann, K., & Arroyo , L. (1989). *Introducción al derecho penal y al derecho penal procesal*. Córcega: Ariel S. A. .
- Shahzad, H., Rustam, F., Flores, E., Vidal, J., De la Torre, I., & Ashraf, I. (16 de junio de 2022). *Multidisciplinary Digital Publishing Institute*. Obtenido de Una revisión de las

técnicas de procesamiento de imágenes para deepfakes:

<https://doi.org/10.3390/s22124556>

Sierra , Y. (1 de agosto de 2023). *Legaltech*. Obtenido de Derecho tecnológico o informático:

qué es, ejemplos y clasificación: <https://blog.lemontech.com/derecho-tecnologico-o-informatico->

definicion/#:~:text=La%20diferencia%20entre%20derecho%20inform%C3%A1tico%20y%20la%20inform%C3%A1tica%20jur%C3%ADdica%20es,se%20le%20conoce%20como%20legaltech.

Suñe, E. (2017). *Dereho informático: Informática Jurídica y Derecho de la Informática*.

Téllez Valdés, J. (2009). *Derecho Informático*. México: McGraw-Hiall. . <https://doi.org/4ta>.

Edición

TN University . (2024). *Diccionario sobre Inteligencia Artificial*. Hermosillo: TN Editorial.

University of Advanced Technologies. (9 de diciembre de 2019). *UNIAT* . Obtenido de

FaceApp con inteligencia artificial: <https://www.uniat.edu.mx/faceapp/>

Urbina, G. (2017). *Introducción a la seguridad informática*. Grupo editorial PATRIA.

Weitzman, C. (26 de enero de 2024). *Los 7 mejores creadores de vídeos deepfake*.

Obtenido de Speechify: <https://speechify.com/es/blog/los-mejores-falsificadores-de-video/#:~:text=DeepFaceLab%20es%20un%20software%20de,v%C3%ADdeos%20falsos%20de%20alta%20calidad>.

Yuchen Jiang, X. (07 de Marzo de 2022). *SPRINGER LINK*. Obtenido de

<https://link.springer.com/article/10.1007/s44163-022-00022-8>

11. Anexos

Anexo Nro. 1. Memorando de designación del Director del Trabajo de Integración Curricular o Titulación



UNL | Universidad
Nacional
de Loja

Carrera de
Derecho

Memorando Nro.: UNL-FJSA-CD-2024-0507-M

Loja, 06 de mayo de 2024

PARA: Sr. Guilber Rene Hurtado Herrera
Docente Titular Auxiliar 1

Sra. Ena Regina Pelaez Soria
Secretaria Abogada

ASUNTO: DESIGNACION DE DIRECTOR TIC DE EVELYN DEL CARMEN
VARGAS GRANDA

Una vez que el día de hoy, 06 de mayo de 2024, a las 13 horas 00 minutos, se ha recibido la petición presentada por la señorita **EVELYN DEL CARMEN VARGAS GRANDA**, estudiante del octavo ciclo; acogiendo lo establecido en el **Art. 228 Dirección del trabajo de integración curricular o de titulación**, del Reglamento de Régimen Académico de la UN vigente; una vez emitido el informe favorable de estructura, coherencia y pertinencia del proyecto; me permito designarlo como **DIRECTOR del Trabajo de Integración Curricular o Titulación**, titulado: **“LA MANIPULACIÓN DE ARCHIVOS DE VIDEO, IMAGEN O VOZ UTILIZANDO LA INTELIGENCIA ARTIFICIAL VULNERA EL DERECHO A LA INTIMIDAD PERSONAL Y FAMILIAR”**, de autoría del antes mencionado estudiante.

Se le recuerda que conforme lo establecido en el Art. 228 del RRA-UNL, usted en su calidad de directora del trabajo de integración curricular o de titulación *“será responsable de asesorar y monitorear con pertinencia y rigurosidad científico-técnica la ejecución del proyecto y de revisar oportunamente los informes de avance, los cuales serán devueltos al aspirante con las observaciones, sugerencias y recomendaciones necesarias para asegurar la calidad de la investigación. Cuando sea necesario, visitará y monitoreará el escenario donde se desarrolle el trabajo de integración curricular o de titulación”*.

Por la atención dada, le expreso mi sincero agradecimiento

C.C. Sr/Srta EVELYN DEL CARMEN VARGAS GRANDA
Expediente De Estudiante
Archivo

Atentamente,



UNL

Universidad
Nacional
de Loja

Carrera de
Derecho

Memorando Nro.: UNL-FJSA-CD-2024-0507-M

Loja, 06 de mayo de 2024

Documento firmado electrónicamente

Sr. Mario Enrique Sanchez Armijos
DIRECTOR DE CARRERA

Anexos:

- evelyn_vargas_-_proyecto_de_integración_curricular.pdf

cycc



Firmado electrónicamente por:
MARIO ENRIQUE
SANCHEZ ARMIJOS

* Documento firmado electrónicamente por SIdoc

Educamos para **Transformar**
2/2

Anexo Nro. 2. Formato de Encuesta



UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENCUESTA DIRIGIDA A PROFESIONALES DEL DERECHO, CONOCEDORES DEL PROBLEMA Y ESPECIALISTAS EN INFORMÁTICA

Distinguido/a: Me encuentro realizando mi Trabajo de Integración Curricular previo a la obtención del Título de Abogada. El tema que estoy desarrollando es el siguiente: “La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”. Para avanzar en esta investigación, solicito su valioso aporte a través de la presente encuesta. La información recabada es únicamente con fines académicos y será tratada con la debida confidencialidad. De antemano le agradezco por participar en esta encuesta.

Problema de investigación: En la era actual, la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial plantea amenazas a la veracidad de la información. Aunque esta tecnología ofrece avances prometedores, su mal uso vulnera derechos fundamentales como lo es el derecho a la intimidad personal y familiar. En nuestro marco legal, el COIP tipifica delitos en el ámbito digital, mientras que en México se han aprobado reformas penales para prevenir el uso indebido de la Inteligencia Artificial.

ENCUESTA

1. Estima usted que con la manipulación de archivos de video, imagen o voz mediante la Inteligencia Artificial se afecta principalmente:

- a) Derecho a la intimidad personal y familiar.

- b) Derecho al honor y buen nombre.
- c) Derecho a la protección de datos de carácter personal.
- d) Derecho a la verdad.

¿POR QUÉ?

.....
.....
.....
.....

2. ¿Cree usted que el uso de la Inteligencia Artificial en la manipulación archivos de video, imagen o voz afecta gravemente el derecho a la intimidad personal y familiar?

SI () NO ()

¿POR QUÉ?

.....
.....
.....
.....

3. ¿Estima usted que la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar?

SI () NO ()

¿POR QUÉ?

.....
.....
.....
.....

4. ¿Está usted de acuerdo en tipificar y sancionar en la legislación penal ecuatoriana la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial para garantizar el derecho a la intimidad personal y familiar?

SI () NO ()

¿POR QUÉ?

.....
.....
.....
.....

5. ¿Cree usted necesario que se realicen campañas de concientización para educar a la sociedad sobre los riesgos de la manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial?

SI () NO ()

¿POR QUÉ?

.....
.....
.....
.....

Anexo Nro. 3. Formato de entrevistas.



UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENTREVISTA DIRIGIDA A PROFESIONALES DEL DERECHO, CONOCEDORES DEL PROBLEMA Y ESPECIALISTAS EN INFORMÁTICA

Distinguido/a: Me encuentro realizando mi Trabajo de Integración Curricular previo a la obtención del Título de Abogada. El tema que estoy desarrollando es el siguiente: “La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”. Para avanzar en esta investigación, solicito su valioso aporte a través de la presente entrevista.

Problema de investigación: En la era actual, la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial plantea amenazas a la veracidad de la información. Aunque esta tecnología ofrece avances prometedores, su mal uso vulnera derechos fundamentales como lo es el derecho a la intimidad personal y familiar. En nuestro marco legal, el COIP tipifica delitos en el ámbito digital, mientras que en México se han aprobado reformas penales para prevenir el uso indebido de la Inteligencia Artificial.

ENTREVISTA

1. Según su criterio ¿Cuáles son las afectaciones adicionales al derecho a la intimidad personal y familiar que se dan como consecuencia de la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial?

.....
.....
.....
.....

2. ¿Considera usted que hay vulneración a la intimidad personal y familiar como consecuencia de la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial?

.....
.....
.....
.....

3. ¿Cree usted que la falta de tipificación y sanción de la manipulación de archivos de video, imagen o voz mediante la utilización de la Inteligencia Artificial contribuye a la vulneración del derecho a la intimidad personal y familiar?

.....
.....
.....
.....

4. ¿Estima usted que tipificando y sancionando en la legislación penal ecuatoriana la manipulación de archivos de video, imagen o voz a través del uso de la Inteligencia Artificial se garantiza el efectivo goce del derecho a la intimidad personal y familiar?

.....
.....
.....
.....

5. ¿Qué otras soluciones sugieren usted frente al problema planteado?

.....
.....
.....
.....

6. ¿Qué medidas considera necesarias para concienciar a la sociedad sobre los riesgos asociados a la manipulación de archivos de video, imagen o voz mediante el uso de la Inteligencia Artificial en el contexto de las nuevas tecnologías en la actualidad?

.....

.....

.....

.....

Anexo Nro. 4. Certificación del Abstract.

Loja, 1 de agosto de 2024

Lorena Patricia Sinche Salinas con número de cédula 1104990450, Magíster en Enseñanza del idioma inglés como Lengua Extranjera, con registro de la SENESCYT número 1021-2021-2363754.

CERTIFICO:

Haber realizado la traducción textual correspondiente al resumen del trabajo de titulación: **“La manipulación de archivos de video, imagen o voz utilizando la Inteligencia Artificial vulnera el derecho a la intimidad personal y familiar”** de autoría de **Evelyn del Carmen Vargas Granda**, con número de Cédula: **1150648739**

Es todo lo que puedo certificar en honor a la verdad, facultando al portador el presente documento para el trámite correspondiente.



Mgtr. Lorena Patricia Sinche Salinas

Cédula: 1104990450

E-mail: lory.sinche@gmail.com

Anexo Nro. 5. Aptitud legal



FACULTAD, JURIDICA SOCIAL Y ADMINISTRATIVA
SECRETARÍA GENERAL

DECLARATORIA DE APTITUD DE TITULACIÓN.

PhD.
Paulina Moncayo Cuenca.
DECANA DE LA FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA.

RESUELVO:

Conocido el informe No. UNL-FJSA-SG-2024-0778 de 27 de septiembre de 2024, emitido por la Dra. Ena Regina Peláez Soria, Secretaria Abogada de la Facultad, en el que se establece que la **Srta. VARGAS GRANDA EVELYN DEL CARMEN** de nacionalidad ecuatoriana, con cédula Nro. **1150648739**, ha cumplido con los requisitos establecidos en el Art. 235 del Reglamento de Régimen Académico de la UNL en vigencia; me permito resolver:

Declaro la **APTITUD DE TITULACIÓN**, previo a la obtención del Título de **ABOGADA** en favor de la **Srta. VARGAS GRANDA EVELYN DEL CARMEN**.

Notifíquese con el presente a la interesada.

Loja, 27 de septiembre de 2024.



ROSARIO PAULINA
MONCAYO CUENCA

PhD. Paulina Moncayo Cuenca.
**DECANA DE LA FACULTAD JURÍDICA,
SOCIAL Y ADMINISTRATIVA.**

C.C. **Vargas Granda Evelyn del Carmen.**
Carrera de Derecho.
Secretaría General.
Expediente estudiantil.



KARINA PAOLA ROJAS
JARAMILLO

Elaborado por: Abg. Karina Rojas J.