UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

"La responsabilidad legal en casos de extorsión por difusión de imágenes generadas por inteligencia artificial"

Trabajo de Titulación para optar la obtención del Título de Abogada de los Tribunales y Juzgados de la República del Ecuador

Autora:

Pacheco Tapia Karla Lisseth

Tutor:

Mgs Campuzano Llaguno Rosita Elena.

Riobamba, Ecuador. 2025.

DECLARACIÓN EXPRESA DE AUTORÍA

Yo, Karla Lisseth Pacheco Tapia, con cédula de ciudadanía 0650076524, autora del trabajo de investigación titulado "LA RESPONSABILIDAD LEGAL EN CASOS DE EXTORSIÓN POR DIFUSIÓN DE IMÁGENES GENERADAS POR INTELIGENCIA ARTIFICIAL", certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mi exclusiva responsabilidad. Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autora de la obra referida será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 9 de junio de 2025.

Karla Lisseth Pacheco Tapia.
C.I.: 0650076524
AUTORA

DICTAMEN FAVORABLE DEL TUTOR

Quien suscribe, **Rosa Elena Campuzano** catedrática adscrita a la Facultad de Ciencias Políticas y Administrativas, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: **"LA RESPONSABILIDAD LEGAL EN CASOS DE EXTORSIÓN POR DIFUSIÓN DE IMÁGENES GENERADAS POR INTELIGENCIA ARTIFICIAL"**, bajo la autoría de **KARLA LISSETH PACHECO TAPIA**; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba a los 6 días del mes de mayo de 2025.

Dra. Rosa Elena Campuzano Llaguno.

TUTORA DEL PROYECTO

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación, "La responsabilidad legal en casos de extorsión por difusión de imágenes generadas por Inteligencia Artificial", presentado por Karla Lisseth Pacheco Tapia, con cédula de identidad número 0650076524, bajo la tutoría del Dra. Rosita Campuzano; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, Riobamba 10 de junio del 2025.

Dr. Segundo Walter Parra Molina.

PRESIDENTE DEL TRIBUNAL DE GRADO

Dr. Nelson Francisco Freire Sánchez.

MIEMBRO DEL TRIBUNAL DE GRADO

Mgs. Wendy Pilar Romero Noboa.
MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICACIÓN

Que, **PACHECO TAPIA KARLA LISSETH** con CC: **0650076524**, estudiante de la Carrera de **DERECHO**, Facultad de **CIENCIAS POLITICAS Y ADMINISTRATIVAS**; ha trabajado bajo mi tutoría el trabajo de investigación titulado **"LA RESPONSABILIDAD LEGAL EN CASOS DE EXTORSION POR DIFUSION DE IMÁGENES GENERADAS POR INTELIGENCIA ARTIFICIAL"**, cumple con el 3%, de acuerdo al reporte del sistema Anti plagio **COPILOT**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 29 de abril de 2025.

Dra. Rosita Campuzano.
TUTORA

DEDICATORIA

El presente trabajo de investigación se lo dedico a Dios, a mi madre Marcia que día a día luchó conmigo en el camino, acompañándome en cada paso de mi vida de estudiante, a mi Abuelita Martha que me apoyo y me tuvo en sus oraciones, a mi tío Diego que fue la persona que me apoyo en el estudio y el apoyo emocional para terminar la carrera, a mi tío Geovanny quien ha sido un padre para mí y me alentó a llegar hasta el final, a mi tío Jorge quien nunca me dejo, a mis hermanas que me inspiraron en cada paso, a mi Marujita mi bis abuelita que ha sido una amiga incondicional y a mis sobrinos y primos que me impulsaron a seguir, también para mis mascotas que muchas veces sin hablar me dieron ánimos y ayudaron a levantarme.

Los amo y admiro tanto. Gracias por creer en mí. Siempre serán mi mayor inspiración.

Karla Lisseth Pacheco Tapia.

AGRADECIMIENTO

Agradezco a Dios por guiar mis pasos, por darme la oportunidad de seguir y disfrutar de esta gran experiencia. A mi madre Marcia, quien estuvo conmigo y me apoyo en todas las decisiones que tomaba, quien muchas veces se desveló conmigo para cumplir esta gran meta, gracias por apoyarme en todo momento y no dejarme rendir durante el proceso. A mi abuelita quien sin muchas veces entender mis angustian y preocupaciones de estudiante me apoyo y me tuvo en sus oraciones le admiro mucho, a mi bisabuelita que siempre me ha hecho reír y recordar quien soy.

A mis tíos, por ser más que nada mis protectores, por darme el estudio y apoyarme moral y económicamente quien a pesar de la distancia me acompaño a diario en mis estudios y nunca permitió que me rinda, me han ayudado a construir mi futuro y me da el ejemplo de no rendirme nunca, sin duda alguna son los hombres de mi vida.

A mis hermanas, por su motivación y apoyo, gracias por iluminar mi vida, aunque somos mundos diferentes cada una de ustedes me han hecho ser quien soy y todas han limpiado mis lagrimas sanando mi corazón manteniéndome de pie en este camino.

A mis sobrinos, gracias por hacerme sentir una niña a su lado por incluirme a sus locuras y ser mi botana de aire fresco cuando sentía que me ahogaba, a mis primos que aunque están lejos y les vea poco tiempo les siento cerca de mi corazón son un regalo a quienes les extraño mucho. Los amo más allá de las palabras.

A mis mascotas que sin hablar para me dijeron mucho con su amor y a mis mascotitas que están en el cielo y me acompañaron hasta cuando estuvieron.

Karla Lisseth Pacheco Tapia.

ÍNDICE GENERAL

INDICE DE GRÁFICOS

RESUMEN

Esta tesis explora la responsabilidad legal en situaciones de extorsión donde se utilizan imágenes creadas con inteligencia artificial (IA). Este fenómeno, que representa un reto creciente en el ámbito legal, plantea interrogantes sobre cómo las leyes actuales pueden abordar delitos relacionados con la creación y difusión de imágenes falsas con fines de extorsión. El objetivo principal de esta investigación es evaluar las implicaciones jurídicas de la tecnología de IA en estos casos y proponer modificaciones al marco legal para enfrentar estos nuevos delitos. La investigación se llevó a cabo mediante un enfoque cualitativo, que incluyó un análisis detallado de las leyes vigentes y la revisión de casos judiciales relacionados con extorsión y delitos informáticos. Además, se realizaron entrevistas con expertos en derecho y tecnología para comprender mejor los retos legales. Esta práctica consiste en crear y utilizar imágenes falsas para chantajear a individuos, aprovechando avances tecnológicos como las redes generativas adversariales. La legislación en muchos países, incluido Ecuador, no está actualizada para abordar estas nuevas formas de ciberdelito, lo que deja a las víctimas desprotegidas y a los perpetradores sin sanciones claras. También se destaca la importancia de implementar medidas preventivas y formar adecuadamente a los profesionales del derecho para garantizar una protección efectiva de las víctimas.

Palabras claves: Extorsión digital-Imágenes generadas por inteligencia artificial (IA)-Ciberdelitos - Derecho comparado-Ética -Seguridad

ABSTRACT

This thesis explores legal liability in extortion cases involving images created with artificial intelligence (AI). This phenomenon, which represents a growing challenge in the legal field, raises questions about how current laws can address crimes related to the creation and dissemination of false images for extortion purposes. The main objective of this research is to assess the legal implications of AI technology in such cases and to propose modifications to the legal framework to address these emerging crimes. The research was conducted using a qualitative approach, which included a detailed analysis of existing laws and a review of court cases related to extortion and cybercrime. In addition, interviews were conducted with legal and technology experts to gain a better understanding of the legal challenges. This practice involves creating and using false images to blackmail individuals, taking advantage of technological advances such as generative adversarial networks. Legislation in many countries, including Ecuador, is not updated to address these new forms of cybercrime, leaving victims unprotected and perpetrators without clear sanctions.

The thesis also highlights the importance of implementing preventive measures and properly training legal professionals to ensure effective protection for victims.

Keywords: Digital extortion – AI-generated images – Cybercrime – Comparative law – Ethics – Security

Tatiana Elizabeth Martinez Zapata

Reviewed by:
Mgs. Tatiana Martínez Zapata
ENGLISH PROFESSOR
C.C: 0605777192

CAPÍTULO I. INTRODUCCIÓN

La extorsión a través de imágenes creadas con inteligencia artificial se ha convertido en un problema creciente en el mundo digital actual. Esta práctica consiste en usar fotos íntimas o comprometedoras, generadas o manipuladas con tecnología, para amenazar a una persona con hacerlas públicas, con el fin de obtener dinero o ejercer algún tipo de control según lo investigado por Gómez en 2024.

La falta de una base legal en Ecuador para abordar el problema de la extorsión por la difusión de imágenes creadas por inteligencia artificial es una cuestión que requiere una inmediata atención. Este vacío en la normativa complica la defensa de los derechos de las personas afectadas y así también en la definición clara de las responsabilidades legales tanto de los infractores como de los proveedores de servicios en línea y en vista de esta falta de medidas adecuadas y efectivas ante estos problemas que se dan con este nuevo ámbito tecnológico y digital como los ciberdelitos y la protección de datos personales frente al uso de la inteligencia artificial; se hace relevante establecer políticas y regulaciones que den protección y seguridad en estas cuestiones de forma integral. Es cada vez más importante que se trabaje dentro del mismo para crear un entorno digital más seguro y confiable para la sociedad. Como lo mencionan Véliz y Chavez (2024), no basta con solo tener leyes es también clave educar y generar conciencia sobre el uso responsable y seguro de las redes sociales y plataformas digitales que hoy en día es una herramienta de nuestro diario vivir ya que esto puede ayudar a prevenir muchos delitos informáticos.

Este tema se expone en cómo debe responder el Derecho cuando se usa inteligencia artificial para compartir imágenes íntimas sin el consentimiento de la persona afectada y el cómo se debe dar solución legal. Esto se trata de una forma de extorsión que está generando desafíos importantes para nuestra sociedad y aun mas para el Derecho donde debe hallar una manera de cuidar y preservar los derechos que tenemos como ciudadanos, con el avance de estas tecnologías, es urgente analizar las leyes que ya existen y considerar la creación de nuevas leyes y políticas que realmente protejan a las víctimas y aseguren que quienes cometen estos actos enfrenten consecuencias justas para así tener

confianza en el sistema legal al acudir por algún motivo de estos. (Moncayo Vives & Vélez Ponce, 2024)

En el año 2018, Perú dio un paso importante e impactante en la protección digital

de las personas al convertir en delito la divulgación de contenido íntimo sin consentimiento en el cual también viene de la mano la Inteligencia artificial en la creación de la misma, por eso la nueva legislación busca proteger la privacidad y dignidad de las personas frente al acoso y la violación de su intimidad, a la vez a la exposición de la extorsión a la vulneración de estos derechos.

El Decreto Legislativo N°1410 de Perú amplió el Código Penal para sancionar conductas como el acoso virtual, el chantaje sexual y la difusión no autorizada de imágenes o audios con contenido sexual. La ley nos dice que al compartir material íntimo sin permiso es un grave error que tendrá consecuencias legales, es aquí donde entra la generación de imágenes sin su consentimiento y a la vez la exhibición a que se de un chantaje mediante esta creación de la imagen.

En Ecuador el Art. 103 del Código Integral Penal nos habla sobre Pornografía con utilización de niñas, niños o adolescentes enfatizando que con la Inteligencia artificial se puede crear imágenes a partir de las fotos de estos niños y así difundirla ilegalmente aquí nos dice que "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; será sancionada con pena privativa de libertad de trece a dieciséis años". Aquí nos dice que la persona que produzca trasmita o edite materiales con fines sexuales siendo reales o simulados de todas maneras será sancionado, aquí podríamos incluir a la I.A como instrumento para la realización de este material.

Nadie tiene derecho a exponer tu vida privada sin tu consentimiento en casos de extorsión o chantaje relacionados con imágenes íntimas, los responsables podrían enfrentar penas adicionales. Por ejemplo:

Si alguien intenta chantajear a una menor con imágenes íntimas, se estaría cometiendo un delito de extorsión o chantaje, a la difusión de contenido sexual se le añadiría la extorsión por estas imágenes (Barredo et al.2021).

La investigación se aplicó en la provincia de Chimborazo, cantón Riobamba, se centra en la responsabilidad legal en casos de extorsión mediante la difusión de imágenes generadas por I.A., analizando cómo las leyes actuales pueden proteger a las víctimas y qué cambios podrían ser necesarios. Nos interesa entender cómo se maneja legalmente este tipo de extorsión y qué medidas se pueden tomar para prevenirla y castigarla efectivamente.

Para llevar a cabo este estudio, se utilizó varios métodos de análisis, incluyendo el inductivo, el histórico lógico, el dogmático y el descriptivo. Como se trata de una investigación jurídica, adoptó un enfoque cualitativo, basado en la revisión de documentos y en el trabajo de campo que describe y analiza la situación actual. Involucramos a expertos en Derecho digital, abogados especializados en delitos cibernéticos, a quienes se les realizaron preguntas específicas para conocer sus opiniones y experiencias.

En este sentido, se exploró también el enfoque del Derecho comparado, examinando las legislaciones en relación con la extorsión y el uso indebido de imágenes generadas por IA. Comprender cómo otros sistemas jurídicos abordan estas cuestiones proporcionó una perspectiva enriquecedora para el análisis de la legislación ecuatoriana, su estudio comparativo permitió identificar mejores prácticas y posibles ajustes para fortalecer el marco legal ecuatoriano.

1.1 Planteamiento del Problema

Con el avance de la tecnología y sabiendo que la I.A. está tomando un lugar importante en la actualidad, con esto ha surgido un nuevo tipo de amenaza que es la creación de imágenes falsas o manipuladas que pueden ser utilizadas para extorsionar a las personas. Este fenómeno ha dado un salto agigantado en la última década debido a la mejora en las técnicas de IA, como las redes generativas adversariales, que permiten crear imágenes realistas sin la necesidad de una fuente original (Cohen et al., 2020). Estos avances han dejado a los sistemas legales tradicionales luchando y acoplándose por mantenerse al día con las nuevas formas de ciberdelitos que explotan la tecnología para dañar a las personas.

La legislación en muchos países, incluido Ecuador, no aborda de manera específica los delitos relacionados con la extorsión mediante imágenes generadas por IA. las leyes que existentes sobre extorsión y privacidad a menudo no consideran las complejidades y retos que es al ser introducidas por la IA, lo que crea vacíos legales que pueden ser explotados por los delincuentes (Smith & Anderson, 2021). Los sistemas

judiciales enfrentan desafíos en la identificación y persecución de estos delitos, ya que la naturaleza digital y la anonimidad proporcionada por la IA dificultan la atribución y el rastreo de los perpetradores.

Es probable que en un futuro la utilización de herramientas de IA aún más avanzadas incremente los casos de extorsión mediante imágenes falsas. Sin una actualización adecuada del marco legal, estos delitos seguirán en aumento, con implicaciones graves para la privacidad y la seguridad de los individuos. Los legisladores deberán trabajar rápidamente para desarrollar regulaciones que aborden específicamente el uso de I.A. en la creación de imágenes con fines extorsivos, incluyendo medidas preventivas y sanciones claras. (Kerr, 2022).

La investigación se centrará en analizar la responsabilidad legal en casos de extorsión mediante la difusión de imágenes generadas por IA, evaluando cómo las leyes actuales pueden proteger a las víctimas y qué cambios deben ser necesarios para abordar estas nuevas formas de delito. Se investigarán los vacíos legales existentes en la legislación ecuatoriana y se compararán con las regulaciones en otros países, para identificar mejores prácticas y posibles ajustes legislativos (Jones, 2023). El objetivo es proponer recomendaciones para fortalecer el marco legal ecuatoriano y mejorar la respuesta judicial ante estos nuevos delitos.

1.2 Justificación

La extorsión por difusión de imágenes generadas por inteligencia artificial es un problema creciente en esta era digital donde cada día es un paso para la tecnología y el cual implica el uso de imágenes íntimas o comprometedoras de una persona para chantajearla y obtener beneficios económicos o control sobre ella ante. Ante esta problemática existente es fundamental contar con un marco legal sólido que proteja los Derechos de las víctimas y establezca las responsabilidades legales de los infractores en este trabajo se analizarán las leyes de protección de datos personales, la legislación sobre delitos informáticos y las normativas relacionadas con la I. A., así como las responsabilidades penales de los extorsionadores. La difusión de contenido íntimo no consentido a través de la I. A. planteará nuevos retos en el ámbito jurídico ya que viene de la mano con la extorsión que viene con ellos al tener en el poder una imagen generada por I.A para contenido sexual sea para su difusión o para generar miedo. Esto debe incluir la revisión de leyes y regulaciones existentes urgentemente para frenar la mala utilización de la tecnología y de la I.A, así como la discusión sobre la necesidad de crear marcos

legales y políticas específicas para proteger a las víctimas y responsabilizar a los perpetradores de este tipo de delitos ya que existen aún vacíos.

1.3 Objetivos

1.3.1 Objetivo General

Analizar la responsabilidad legal en casos de extorsión por difusión de imágenes generadas por I. A., para identificar los vacíos en la legislación ecuatoriana sobre delitos cibernéticos.

1.3.2 Objetivos Específicos

- Conocer los fundamentos teóricos y legales relacionados con la extorsión y el uso de imágenes generadas por I. A., analizando la doctrina y jurisprudencia existente para establecer un marco conceptual sólido que sustente el estudiar de la legislación ecuatoriana.

- Determinar la influencia del uso de imágenes generadas con inteligencia artificial relacionadas con el delito de extorsión en el Ecuador con el fin de identificar áreas de mejora en la legislación.

- Comprender los tipos de extorsión vinculados a la difusión de imágenes generadas por inteligencia artificial, mediante un enfoque de derecho comparado que examine legislaciones internacionales sobre delitos cibernéticos y protección de datos, con el propósito de identificar prácticas y normativas efectivas que puedan ser aplicadas o adaptadas en Ecuador para fortalecer la protección de las víctimas y mejorar la respuesta legal frente a estos delitos.

CAPÍTULO II. MARCO TEÓRICO

2.1. Estado del Arte

Respecto del tema “Responsabilidad legal en casos de extorsión por difusión de imágenes generadas por la I. A.” no se han realizados trabajos investigativos iguales; sin embargo, existen algunos similares al que se pretende realizar, cuyas conclusiones más importantes son las siguientes:

David García Pérez, en Ecuador, evaluó la situación legal del país en el año 2022. Él investigó cómo la ley ecuatoriana aborda la extorsión con imágenes generadas por I. A. García descubrió que la ley actual no protege adecuadamente a las víctimas y que hay aspectos legales que deben ser mejorados para responsabilizar a los delincuentes (García, 2022).

José Luis Martínez Torres, en México, exploró la situación legal mexicana en el año 2021. Él examinó cómo la ley de México trata la extorsión con imágenes generadas por I. A. Descubrió que la ley actual no aborda directamente este problema, lo que deja a las víctimas sin protección clara y permite que los delincuentes evadan responsabilidades (Martínez, 2021).

María González Ruiz y Javier López Sánchez, en España, se adentraron en la jurisprudencia española en el año 2020. Analizaron cómo los tribunales han tratado casos de extorsión con imágenes falsas creadas por I.A, aunque notaron avances en la protección de las víctimas, encontraron áreas donde la ley aún puede mejorar para garantizar una respuesta más justa (González & López, 2020).

Estos estudios resaltan la importancia de actualizar las leyes para abordar adecuadamente la extorsión con imágenes generadas por I. A. y proteger así a las víctimas.

2.2 Aspectos Teóricos

2.2.1 UNIDAD I. Fundamentos de la responsabilidad legal en extorsión por difusión de imágenes generadas por IA.

Según Greenberg (2021), "la capacidad de generar imágenes falsas de manera convincente mediante IA complica la identificación y el procesamiento de casos de

extorsión" (p. 45). Pone al descubierto que la mala utilización de estos pueden

generar un retroceso en la sociedad y aun más vulnera nuestros derechos esto sugiere que los sistemas legales deben adaptarse para abordar estos casos de manera efectiva, garantizando la protección sin obstaculizar la innovación tecnológica que sin duda no podemos frenar y que se esta dando a pasos agigantados, esto debe ser apoyo para nosotros teniendo un buen uso del mismo.

El marco legal actual enfrenta desafíos significativos para abordar la extorsión por imágenes generadas por IA debido a la dificultad para establecer la autenticidad ya que no solo quien genera la imagen tiene responsabilidad si no también la herramienta con la cual se realizó la imagen y el propósito malicioso detrás de la difusión de dichas imágenes. Como señala Smith (2022), "las leyes de difamación y privacidad tradicionales pueden no ser suficientes para proteger a las víctimas de la difusión de imágenes generadas por IA, ya que estas no siempre cumplen con los criterios de difamación convencionales" (p. 112). La tecnología avanza y la sociedad debería ir a la par, lamentablemente esto no se da aun menos en nuestras leyes por ese motivo debe existir una regulación pronta de la misma.

Esta falta de claridad legal puede dejar a las víctimas en una posición vulnerable, con recursos limitados para buscar reparación la responsabilidad legal en casos de extorsión por imágenes sintéticas puede variar según la jurisdicción y la interpretación legal específica de cada país, pero deberíamos saber que la finalidad debe ser la misma, castigar a la persona responsable de vulnerar el derecho y proteger a las personas de estas exhibiciones.

En algunos países, como señala Jones (2023), "se han propuesto leyes específicas que criminalizan la creación y difusión maliciosa de imágenes generadas por IA con el propósito de extorsión" (p. 76). Y se debería tomar en cuenta que esta herramienta la tenemos todos y es muy necesario implementar leyes específicas para la creación y difusión de estas imágenes que no tienen un propósito bueno tomar las precauciones necesarias para no estar expuestos a estas vulneraciones.

Estas leyes buscan llenar vacíos legales y proporcionar un marco claro para la responsabilidad legal en casos cada vez más comunes de abuso tecnológico y es crucial pensar el papel de las plataformas tecnológicas y los proveedores de servicios en la prevención y remisión de la extorsión por imágenes generadas por IA.

Según Davis (2020), "las plataformas de redes sociales y los proveedores de servicios en línea pueden desempeñar un papel activo mediante la implementación de políticas de uso responsable y mecanismos de denuncia efectivos" (p. 231). Las redes sociales se ha vuelto común entre todos es por eso que se debería tomar en cuenta que es en esos lugares donde se debe incluir más formas de protección.

Tienen la responsabilidad de proteger la integridad de sus usuarios y deben colaborar con las autoridades para abordar adecuadamente los casos de abuso y el desarrollo de políticas y legislaciones efectivas es fundamental para abordar los desafíos emergentes relacionados con la extorsión por imágenes generadas por IA.

Como menciona Brown (2021), trabajar en conjunto a nivel internacional y unificar ciertas normas legales puede ayudar a cerrar vacíos en las leyes y a dar una respuesta más fuerte y coordinada frente a estos problemas (p. 198). Esto muestra claramente que no basta con tener leyes nacionales, sino que también hace falta colaboración entre países para enfrentar de forma más completa los riesgos que trae el uso indebido de nuevas tecnologías como la inteligencia artificial.

En el caso de la extorsión a través de imágenes creadas por IA, nos encontramos con una situación muy delicada. Estas imágenes pueden parecer completamente reales, aunque nunca hayan sido tomadas en la vida real. Además, pueden crearse sin que la persona afectada lo sepa o lo autorice, lo que hace que el daño sea aún más serio. Por eso, es urgente que las leyes se actualicen y que también existan acuerdos entre países para regular mejor estas prácticas y proteger a las personas que podrían ser víctimas.

2.2.1.1 ¿Qué son realmente las imágenes generadas por IA?

Para entender bien este tipo de casos, primero hay que saber cómo funcionan estas imágenes. Se trata de contenido visual creado por inteligencia artificial, muchas veces con una calidad tan alta que cuesta diferenciar si es real o no. A veces se les llama imágenes sintéticas o deepfakes, y se generan a partir de datos que la máquina va aprendiendo, hasta lograr un resultado muy realista.

Una técnica muy usada para esto es la de redes adversarias, como explican Goodfellow y otros (2014). Básicamente, se usan dos sistemas que “compiten” entre sí: uno crea las imágenes y otro intenta detectar si son falsas, y así el primero va mejorando hasta que el segundo ya no puede notar la diferencia (p. 1578).

El gran problema con estas imágenes es que pueden parecer tan reales como una foto de verdad. Esto hace muy difícil saber si han sido manipuladas, sobre todo cuando se usan con malas intenciones. Como dicen Li y sus colegas (2018), este tipo de imágenes puede ser casi imposible de distinguir de una fotografía auténtica, lo que complica mucho las cosas tanto a nivel social como legal (p. 932).

Tener claro qué es una imagen creada por IA y cómo se diferencia de una real es clave. Bartneck y Suzuki (2020) señalan que esa definición clara es necesaria para poder establecer quién es responsable cuando se usan estas imágenes de forma dañina y para decidir qué reglas se deben aplicar (p. 45).

A medida que pasa el tiempo, estas tecnologías se vuelven más avanzadas. Tan y su equipo (2021) explican que, gracias al aprendizaje automático, las imágenes creadas por IA son cada vez más detalladas y realistas, tanto que pueden engañar fácilmente a quien las ve si no sabe cómo reconocerlas (p. 764).

Estas imágenes pueden usarse en muchos ámbitos: desde el arte y la publicidad, hasta campañas de desinformación o incluso chantaje. Nguyen et al. (2019) mencionan que son muy versátiles y que pueden aparecer en áreas tan diferentes como el entretenimiento, la ciencia o el marketing (p. 220). Pero justamente por eso, también es más difícil controlar su uso y asegurar que se empleen de forma ética.

Comprender bien cómo funcionan estas imágenes es básico para poder prevenir su uso con fines negativos. Liu y Deng (2020) dicen que hace falta seguir investigando en formas de detectar y verificar si una imagen ha sido creada por IA, y que estas herramientas pueden ser muy útiles para frenar la manipulación de contenido (p. 112).

2.2.1.2 ¿Cómo se crean imágenes falsas con inteligencia artificial?

Las imágenes creadas con inteligencia artificial (IA) se generan a través de modelos muy avanzados que aprenden a partir de muchas fotos reales. Uno de los métodos más comunes para hacerlo son las redes neuronales conocidas como Generative Adversarial Networks o GANs. Estas redes funcionan con dos sistemas que “trabajan en equipo”:

El primero se llama “Generador”, y su tarea es crear imágenes falsas usando patrones que ha aprendido.

El segundo se llama “Discriminador”, y su función es detectar cuáles imágenes son reales y cuáles no.

Ambos sistemas se entrenan entre sí: el generador mejora cada vez más hasta que consigue crear imágenes que engañan al discriminador, haciéndolas parecer totalmente reales. Así es como se pueden crear fotos de personas que no existen o modificar imágenes reales de forma muy convincente. El problema surge cuando esta tecnología se usa con malas intenciones, como por ejemplo para chantajear o amenazar a alguien.

Algunas de las aplicaciones más populares que permiten crear este tipo de contenido fueron diseñadas con fines positivos, pero pueden usarse de manera incorrecta para engañar o manipular a otras personas. Aquí algunos ejemplos:

- DeepFaceLab: es una herramienta muy usada para crear deepfakes, cambiando el rostro de una persona por el de otra en fotos o videos. Aunque originalmente se creó con fines de entretenimiento, ha sido usada en casos de sextorsión, ya que puede simular a una persona en situaciones comprometedoras.
- FaceApp: es bastante conocida por sus filtros que permiten cambiar la edad, el género o la expresión facial. Aunque no genera deepfakes avanzados, sí puede alterar fotos de manera que se presten para chantajes o malentendidos.
- Midjourney: esta plataforma permite generar imágenes realistas a partir de descripciones escritas. Si bien se utiliza mucho en diseño y arte digital, también puede emplearse para crear imágenes falsas que simulen situaciones que nunca ocurrieron.
- DALL·E: desarrollada por OpenAI, esta herramienta también convierte texto en imágenes y puede generar contenido visual de alta calidad. Aunque se usa principalmente en proyectos creativos, tiene el potencial de ser usada de forma negativa para fabricar contenido falso.
- Reface: esta app permite poner tu cara en cuerpos de otras personas en gifs o videos. Aunque está pensada para entretenimiento, no se puede ignorar que podría utilizarse con fines maliciosos.

2.2.1.3 ¿Por qué es importante entender esta tecnología desde el derecho?

Conocer cómo funcionan estas aplicaciones es clave para poder hacer leyes que realmente protejan a las personas. Si los legisladores entienden qué se puede hacer con estas herramientas y cuáles son sus límites, será más fácil prevenir su mal uso, crear normas modernas, y proteger a las víctimas.

Además, comprender el lado técnico también ayuda a que las autoridades puedan rastrear de dónde vienen estas imágenes y trabajar junto a las empresas tecnológicas para evitar que este tipo de delitos ocurran o, al menos, que puedan detectarse más fácilmente. Cuanto más sepamos del tema, mejores respuestas podremos dar frente a estas amenazas digitales que siguen creciendo.

2.2.1.4 Precedentes judiciales relevantes sobre extorsión con imágenes creadas por IA

El uso de imágenes generadas por inteligencia artificial ha traído nuevos retos para el derecho, especialmente cuando se utilizan para extorsionar. En Ecuador, este tipo de delitos empieza a ser atendido tanto en la legislación como en los tribunales. Este apartado analiza algunos precedentes importantes sobre cómo se han tratado casos similares, en los que la tecnología se mezcla con delitos ya conocidos, como la extorsión.

La extorsión, en general, implica obtener algo —como dinero o favores— a través de amenazas. Cuando esas amenazas se basan en imágenes creadas con IA, el impacto puede ser aún mayor, porque estas imágenes pueden parecer completamente reales. En Ecuador, la extorsión está regulada por el artículo 185 del Código Orgánico Integral Penal (COIP) (Asamblea Nacional, 2014).

“La extorsión, en el marco de la tecnología, plantea desafíos únicos, ya que las imágenes generadas por IA pueden ser indistinguibles de las reales, lo que incrementa el potencial de daño” (Asamblea Nacional, 2014, p. 32).

Caso internacional: People v. Bollaert (2014) – Estados Unidos

Uno de los casos más conocidos relacionados con extorsión digital ocurrió en California, bajo el nombre People v. Bollaert. Kevin Bollaert fue procesado por crear y administrar el sitio web YouGotPosted, donde se publicaban fotos íntimas de personas sin su permiso, acompañadas de su nombre, dirección y otros datos personales. Además,

Bollaert creó otro sitio, ChangeMyReputation, donde las víctimas debían pagar si querían que sus fotos fueran eliminadas. Este esquema fue considerado claramente como un caso de extorsión y violación a la privacidad. El número del caso es 067863.

Este juicio fue clave porque demostró cómo las leyes tradicionales contra la extorsión y el robo de identidad pueden aplicarse a situaciones nuevas relacionadas con la tecnología. También puso sobre la mesa la necesidad urgente de actualizar la legislación para cubrir estas nuevas formas de abuso digital.

Caso internacional: People v. Bollaert (2014)

El caso People v. Bollaert (2014) marcó un precedente clave en la lucha contra la extorsión digital, especialmente en contextos donde se ven comprometidos derechos fundamentales como la privacidad y la dignidad humana. En este caso, Kevin Bollaert operaba un sitio web que publicaba imágenes íntimas de personas sin su consentimiento, junto con información personal como nombres, perfiles de redes sociales y direcciones. Para eliminar el contenido, las víctimas debían pagar a través de otro sitio vinculado, lo que configuraba un esquema claro de extorsión emocional y económica.

Este juicio demostró que las leyes tradicionales, como las que penalizan la extorsión y el robo de identidad en California, pueden aplicarse con éxito a delitos cometidos en entornos digitales. Sin embargo, también subrayó la necesidad urgente de normativas más específicas que respondan a las nuevas formas de abuso digital.

Uno de los puntos más relevantes de este caso fue que el Tribunal de Apelación de California confirmó la condena de Bollaert por extorsión y uso ilegal de información personal. Además, rechazó que el acusado pudiera ampararse en la Ley de Decencia en Comunicaciones (Communications Decency Act), argumentando que había participado activamente en la creación y difusión del contenido ofensivo. Esto dejó claro que quienes administran plataformas digitales no pueden escudarse en inmunidades legales si ellos mismos generan o fomentan contenido que dañe a terceros.

El fallo judicial dejó sentado que los responsables de plataformas digitales pueden y deben ser considerados legalmente responsables cuando facilitan o promueven la difusión de contenido explícitamente dañino. Esto refuerza la protección del derecho a la intimidad

y traza una línea legal contra prácticas que lucran con la exposición no consentida de datos e imágenes personales.

Más allá del caso específico, People v. Bollaert tuvo un impacto importante en la evolución de la legislación en Estados Unidos, en particular en California, donde a partir de este precedente se fortalecieron leyes contra la "pornografía no consensuada" o revenge porn, reconociendo la gravedad de este tipo de delitos en entornos digitales.

En relación con el uso de inteligencia artificial para generar imágenes falsas con fines de extorsión, este caso aporta una base legal muy valiosa. Aunque el contenido creado con IA agrega una capa de complejidad —al no requerir imágenes reales para dañar a la víctima—, el principio legal sigue siendo similar: se vulneran derechos fundamentales con la intención de obtener un beneficio mediante la coacción. Esto refuerza la necesidad de actualizar nuestras leyes para abordar nuevas amenazas digitales, adaptándolas a los avances tecnológicos que permiten la creación de contenido ficticio con impactos reales sobre las personas.

Precedentes en América Latina

Caso Argentina: Aciar (2016)

En América Latina también se han registrado precedentes importantes. Uno de ellos es el caso Aciar (2016), en Argentina, donde se juzgó la extorsión a través de la difusión no consentida de imágenes íntimas. Aunque no involucraba inteligencia artificial directamente, el caso fue relevante porque permitió aplicar leyes tradicionales de privacidad y extorsión a un entorno digital.

"El caso Aciar en Argentina representa un avance en la protección de las víctimas de extorsión digital, adaptando principios legales tradicionales a nuevas tecnologías" (Cámara Nacional en lo Criminal y Correccional, 2016, p. 7).

Caso Argentina: Aciar (2016)

El caso Aciar, resuelto en 2016 por la Cámara Nacional en lo Criminal y Correccional de Argentina, representó un hito en la adaptación del derecho penal a los delitos digitales. El acusado amenazó a la víctima con divulgar imágenes íntimas sin su consentimiento a menos que accediera a sus exigencias, configurando un claro acto de extorsión digital. El tribunal aplicó disposiciones del Código Penal Argentino sobre

extorsión y violación a la privacidad, pero lo hizo desde una interpretación innovadora que reconocía las nuevas dinámicas del entorno virtual.

Derechos vulnerados:

- Privacidad: La amenaza de difusión de imágenes íntimas sin autorización constituye una violación directa del derecho a la intimidad, protegido tanto por la legislación nacional como por instrumentos internacionales de derechos humanos.
- Integridad moral y psicológica: El acto extorsivo generó un daño emocional severo a la víctima, afectando su estabilidad mental y emocional.
- Honra y reputación: La potencial publicación del contenido amenazaba con dañar gravemente la imagen pública y el entorno social de la víctima.

Autoridad encargada:

La Cámara Nacional en lo Criminal y Correccional fue el tribunal encargado de juzgar el caso, demostrando la capacidad de las leyes penales tradicionales para enfrentar nuevas formas de criminalidad digital mediante un enfoque progresista y contextual.

Precedente judicial:

El fallo fue pionero al evidenciar que los marcos legales existentes pueden aplicarse eficazmente a contextos digitales, extendiendo su alcance más allá del ámbito físico. Este enfoque fortaleció la jurisprudencia en torno a la protección de la intimidad y el combate a la extorsión digital.

Relación con la extorsión mediante imágenes generadas por IA: Si bien en este caso no se utilizó inteligencia artificial, su relevancia reside en que sienta las bases para aplicar principios similares en casos donde se empleen tecnologías avanzadas. La amenaza de divulgar imágenes íntimas generadas por IA también vulnera derechos como la privacidad, la integridad emocional y la reputación, por lo que el razonamiento jurídico del caso Aciar puede extrapolarse a este nuevo tipo de delitos. Este precedente refuerza la urgencia de actualizar el marco normativo para incluir explícitamente el uso de herramientas tecnológicas emergentes en la comisión de delitos.

Caso Brasil: Maria da Penha (2018)

En Brasil, el caso conocido como Maria da Penha digital, resuelto en 2018, constituyó un ejemplo relevante de cómo la legislación contra la violencia de género puede adaptarse para enfrentar la ciberextorsión. En este caso, la víctima fue amenazada con la divulgación de imágenes íntimas, y el tribunal aplicó la Ley Maria da Penha —originalmente diseñada para casos de violencia doméstica y de género— para abordar una forma de violencia digital.

Derechos vulnerados:

- Privacidad: La amenaza de difusión de contenido íntimo sin consentimiento constituyó una violación directa del derecho a la privacidad.
- Integridad emocional y psicológica: La presión ejercida mediante la amenaza tuvo un impacto significativo en la salud mental de la víctima.
- Honra y reputación: La posibilidad de que se publicaran las imágenes afectaba gravemente la dignidad y la percepción social de la víctima.

Autoridad encargada:

El caso fue resuelto por el Supremo Tribunal Federal de Brasil, que interpretó de manera amplia la Ley Maria da Penha para incluir la violencia psicológica ejercida a través de medios digitales. Esto supuso un avance importante en el reconocimiento de la violencia de género en el entorno virtual.

Precedente judicial:

Este caso amplió los alcances de la Ley Maria da Penha, estableciendo que su aplicación no se limita a la violencia física o doméstica, sino que puede cubrir también la violencia digital y psicológica ejercida mediante amenazas y chantajes en línea. Esta ampliación refuerza la necesidad de que los marcos normativos evolucionen junto con las formas contemporáneas de violencia.

Relación con la extorsión por imágenes generadas por IA: Aunque en este caso no se utilizaron imágenes creadas con inteligencia artificial, el precedente es útil para

casos futuros en los que se empleen tecnologías de IA para crear contenido falso con fines extorsivos. La interpretación extensiva de la Ley Maria da Penha demuestra que las herramientas legales diseñadas para proteger a las mujeres frente a la violencia pueden y deben actualizarse para enfrentar nuevos contextos, como la extorsión basada en imágenes manipuladas digitalmente.

Contexto Ecuatoriano y Precedentes Relevantes

En Ecuador, aunque los casos específicos de extorsión mediante imágenes generadas por inteligencia artificial (IA) aún son incipientes, los tribunales han comenzado a reflexionar sobre el impacto de las nuevas tecnologías en el derecho penal. En este contexto, el análisis jurisprudencial y la interpretación evolutiva del marco normativo resultan esenciales para enfrentar los desafíos emergentes (Asamblea Nacional, 2021).

Caso de extorsión cibernética – Corte Constitucional del Ecuador (2021)

Un precedente importante fue establecido por la Corte Constitucional del Ecuador en 2021, en un caso que involucró la amenaza de difundir imágenes comprometedoras obtenidas por medios digitales. El tribunal aplicó las normas tradicionales sobre extorsión al contexto digital, reafirmando la flexibilidad del sistema jurídico ecuatoriano:

"La sentencia de la Corte Constitucional del Ecuador marca un precedente importante en la adaptación de leyes tradicionales de extorsión a contextos digitales, subrayando la flexibilidad del sistema legal" (Corte Constitucional del Ecuador, 2021, p. 23).

Este fallo demuestra cómo la jurisprudencia ecuatoriana comienza a interpretar de manera dinámica el derecho penal frente a las nuevas formas de criminalidad. Lejos de requerir una reforma legislativa inmediata ante cada avance tecnológico, la Corte optó por una lectura expansiva de las normas existentes, reconociendo que las amenazas digitales también constituyen una forma moderna de extorsión. Este enfoque promueve una protección eficaz de los derechos fundamentales sin necesidad de vacíos legales.

La Corte enfatizó que la evolución tecnológica no debe convertirse en refugio para prácticas delictivas, y que la justicia debe seguir siendo capaz de responder, incluso

frente al marco normativo vigente en Ecuador: Responsabilidad penal en casos de extorsión digital

El Código Orgánico Integral Penal (COIP) constituye el principal cuerpo normativo en materia penal en Ecuador. En el contexto de la extorsión y la difusión de información
— incluyendo aquella manipulada mediante IA— el artículo más relevante es el 185, que establece:

"Será sancionada con pena privativa de libertad de cinco a siete años, la persona que obtenga de otra, mediante amenazas, promesas, informaciones falsas o engaños, cualquier beneficio económico o de otra índole" (Asamblea Nacional, 2014, p. 32).

Esta disposición, de redacción amplia, permite abordar situaciones de extorsión en el ámbito digital. Las amenazas pueden involucrar la difusión de contenido manipulado digitalmente, incluyendo imágenes falsas generadas con inteligencia artificial, conocidas como deepfakes. Estas técnicas permiten la creación de contenido altamente realista, cuyo uso indebido puede ocasionar un daño significativo a la imagen, la intimidad o la integridad emocional de la víctima.

El artículo 185 se presenta, por tanto, como una herramienta eficaz para perseguir penalmente este tipo de delitos, ya que contempla la utilización de "informaciones falsas" como medio para obtener beneficios ilícitos. Este aspecto resulta crucial, pues permite incluir dentro del tipo penal la amenaza basada en contenido creado artificialmente con la intención de manipular, extorsionar o humillar a una persona.

2.2.1.5 Retos y desafíos en la aplicación del COIP frente a la extorsión digital

A pesar de contar con una base normativa robusta, existen diversos desafíos para enfrentar eficazmente la extorsión digital en Ecuador:

- Velocidad del avance tecnológico: La rapidez con la que surgen nuevas formas de criminalidad digital, como el uso de IA para crear contenido falso, supera el ritmo de actualización legislativa.
- Dificultades probatorias: La sofisticación de las herramientas digitales complica la identificación del origen del contenido y la verificación de su autenticidad.

- Necesidad de especialización: La investigación y juzgamiento de estos delitos requiere conocimientos específicos en ciberseguridad, verificación de contenido audiovisual y protección de datos personales.

Frente a estos desafíos, es necesario fortalecer la capacitación de jueces, fiscales y operadores del sistema judicial, así como dotarles de herramientas tecnológicas avanzadas. Además, será clave considerar reformas futuras al COIP que reconozcan explícitamente los delitos cometidos con apoyo de IA, sin perjuicio de la aplicabilidad de las normas actuales.

La Ley Orgánica de Protección de Datos Personales de Ecuador, promulgada en 2021, tiene como objetivo salvaguardar los datos personales de los ciudadanos, regulando su tratamiento y estableciendo derechos y obligaciones para quienes los gestionan. Esta legislación es especialmente pertinente en el contexto de la difusión de imágenes generadas por inteligencia artificial (IA), ya que dichas imágenes pueden contener datos personales o sensibles. El tratamiento de estos datos sin el consentimiento explícito del titular constituye una violación de la normativa vigente.

2.2.1.6 Marco Normativo Internacional Comparado con Ecuador

Además de su marco legal interno, Ecuador es parte de diversas convenciones y tratados internacionales que buscan combatir los delitos cibernéticos y proteger los derechos humanos en el ámbito digital.

Convenio de Budapest sobre Ciberdelincuencia: Ecuador es signatario de este tratado internacional, el primero en abordar los delitos cometidos a través de internet y otras redes informáticas. El convenio proporciona un marco legal para la cooperación internacional en la investigación y persecución de delitos cibernéticos, incluyendo la extorsión digital.

Convención Americana sobre Derechos Humanos: También conocida como el Pacto de San José, establece en su artículo 11 el derecho a la privacidad y a la protección de la honra y la reputación. Este principio es aplicable en casos de difusión no consentida de imágenes generadas por IA, que pueden afectar la dignidad y la privacidad de las personas.

2.2.1.7 Legislación Comparada en América Latina

Analizar el marco normativo de otros países de América Latina ofrece perspectivas valiosas para la evolución de la legislación en Ecuador. Países como Argentina, Brasil y México han desarrollado leyes específicas para combatir la extorsión y proteger los datos personales en el entorno digital.

Argentina: La Ley 25.326 de Protección de Datos Personales establece un régimen para la protección de los datos personales y sanciona su uso indebido.

Brasil: La Ley General de Protección de Datos (LGPD) regula el uso de datos personales y establece mecanismos para la protección de la privacidad de los ciudadanos.

México: La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece principios y procedimientos para garantizar la protección de los datos personales y sancionar su uso no autorizado.

Estas legislaciones reflejan un esfuerzo regional por adaptar los marcos legales a los desafíos que presentan las nuevas tecnologías en la protección de la privacidad y los datos personales.

2.2.2 UNIDAD II: ANÁLISIS DE JURISPRUDENCIA Y LEGISLACIÓN COMPARADA

Analicemos cómo diferentes países abordan la problemática de la extorsión digital relacionada con la difusión de imágenes creadas mediante inteligencia artificial (IA), y cómo estas experiencias pueden servir de referencia para Ecuador.

Adaptaciones Legales en Diversos Países

Estados Unidos: Algunos estados han actualizado sus leyes para enfrentar delitos cibernéticos emergentes. Por ejemplo, en California, el Código Penal considera como extorsión las amenazas realizadas mediante contenidos manipulados digitalmente, incluyendo imágenes generadas por IA.

Unión Europea: El Reglamento General de Protección de Datos (GDPR) protege la privacidad de las personas. Los tribunales europeos han determinado que la creación y difusión no autorizada de imágenes alteradas digitalmente violan este derecho y pueden

constituir actos de extorsión.

México y Argentina: Ambos países han incorporado disposiciones para enfrentar delitos cibernéticos. En México, la Ley General de Protección de Datos Personales y el Código Penal Federal incluyen penas por la difusión de contenido falso con fines de extorsión. Argentina, mediante la Ley 26.388 sobre delitos informáticos, sanciona el acceso no autorizado a sistemas informáticos y la extorsión en línea.

Situación en Ecuador

Aunque en Ecuador no existen precedentes judiciales específicos sobre extorsión mediante imágenes generadas por IA, el Código Orgánico Integral Penal (COIP) aborda la extorsión y delitos relacionados. Un ejemplo es la sentencia a dos personas en Quito por extorsionar a una víctima con la difusión de imágenes de contenido sexual.

Además, la Corte Constitucional, en la sentencia No. 2064-14-EP/21, trató sobre la difusión no consentida de imágenes íntimas, enfatizando la protección de la privacidad y la imagen personal.

Consideraciones para Ecuador

Ecuador podría beneficiarse de las experiencias internacionales para fortalecer su marco legal en relación con la extorsión digital y el uso indebido de tecnologías como los deepfakes. Es esencial actualizar las leyes para abordar específicamente estos delitos y garantizar la protección de las víctimas. Además, la cooperación internacional es clave, dado el carácter transnacional de muchos delitos cibernéticos.

La protección de la privacidad y el derecho al honor en el entorno digital son fundamentales. Ecuador podría considerar integrar disposiciones adicionales que

refuercen la protección de la imagen personal en línea y sancionen el uso de tecnologías como los deepfakes para fines extorsivos. Asimismo, es relevante regular la responsabilidad de las plataformas digitales en la gestión y difusión de contenido manipulado, siguiendo ejemplos como el de la Unión Europea.

En Ecuador, el Código Orgánico Integral Penal (COIP) aborda el delito de extorsión en su artículo 185. Este artículo establece que quien, con el fin de obtener un

beneficio propio o para terceros, obligue a otra persona mediante violencia o intimidación a realizar u omitir un acto en perjuicio de su patrimonio o el de otra persona, enfrentará una pena de prisión de tres a cinco años. La sanción aumenta a un rango de cinco a siete años si se presentan circunstancias agravantes, como que la víctima sea menor de edad, mayor de 65 años, mujer embarazada, persona con discapacidad o que padezca enfermedades que comprometan su vida; si el delito es cometido por alguien con quien la víctima tiene una relación laboral o de confianza; si se emplean amenazas graves como de muerte o secuestro; o si el acto se realiza desde un centro de privación de libertad o desde el extranjero.

Además, la Ley Orgánica de Protección de Datos Personales, promulgada en 2021, regula el manejo de la información personal en el país. Esta ley establece que cualquier tratamiento de datos personales debe contar con el consentimiento explícito de su titular y prohíbe su uso para fines ilícitos o sin la autorización correspondiente.

A nivel internacional, Estados Unidos cuenta con la Computer Fraud and Abuse Act (CFAA), una ley federal de 1986 que penaliza el acceso no autorizado a sistemas informáticos y la extorsión mediante la amenaza de divulgar información sensible. Sin embargo, esta legislación ha sido objeto de críticas por su lenguaje ambiguo, lo que ha llevado a interpretaciones amplias y, en ocasiones, a aplicaciones controvertidas.

En el ámbito estatal, California implementó en 2018 la California Consumer Privacy Act (CCPA), otorgando a los residentes derechos significativos sobre sus datos personales. Esta ley permite a los consumidores saber qué información se recopila sobre ellos, solicitar su eliminación y optar por no vender sus datos. Su entrada en vigor marcó un hito en la protección de la privacidad en Estados Unidos, aunque su aplicación ha enfrentado desafíos relacionados con la claridad en los mecanismos de cumplimiento y la necesidad de una regulación federal uniforme.

Comparando con Ecuador, aunque la Ley Orgánica de Protección de Datos Personales representa un avance significativo en la protección de la información personal, aún enfrenta desafíos en su implementación efectiva. La ausencia de una autoridad de protección de datos plenamente operativa y con recursos adecuados podría limitar su eficacia. Además, la legislación ecuatoriana aún no aborda de manera específica delitos emergentes como la extorsión digital o el uso indebido de tecnologías avanzadas, áreas en las que otras jurisdicciones han avanzado más.

Legislaciones latinoamericanas comparadas con Ecuador sobre el delito de extorsión.

En América Latina, varios países han desarrollado marcos legales para proteger los datos personales y abordar delitos como la extorsión, especialmente en contextos digitales. A continuación, se presenta una comparación entre las legislaciones de Argentina, Brasil y Ecuador en relación con la difusión no autorizada de imágenes generadas por inteligencia artificial (IA).

Argentina

Argentina cuenta con la Ley 25.326 de Protección de Datos Personales, que establece un marco claro para la salvaguarda de la información personal de los ciudadanos. Esta legislación reconoce la importancia de proteger la privacidad en el entorno digital y ha sido pionera en la región desde su promulgación en el año 2000. Sin embargo, debido a los avances tecnológicos y la aparición de nuevas amenazas, se ha identificado la necesidad de actualizar esta ley para abordar de manera más efectiva situaciones como la difusión no autorizada de imágenes íntimas, incluyendo aquellas generadas por IA. En este sentido, se han propuesto reformas que buscan incorporar derechos como el de oposición, permitiendo a los ciudadanos rechazar el uso de sus datos para ciertos fines.

Brasil

Brasil implementó en 2020 la Ley General de Protección de Datos (LGPD), inspirada en el Reglamento General de Protección de Datos de la Unión Europea. Esta ley establece normas estrictas sobre el tratamiento de datos personales y ha sido fundamental para abordar desafíos en la era digital. En marzo de 2023, el Tribunal Superior de Justicia de Brasil dictaminó que la filtración de datos personales no genera automáticamente daño moral presunto; es decir, es necesario que la parte perjudicada demuestre el daño sufrido para tener derecho a una indemnización. Este fallo subraya la importancia de la LGPD en la protección de la privacidad y en la adaptación a las nuevas realidades tecnológicas.

Ecuador

Ecuador promulgó en 2021 la Ley Orgánica de Protección de Datos Personales (LOPDP), estableciendo un marco legal para regular el tratamiento de datos personales y proteger la privacidad de sus ciudadanos. Aunque esta ley representa un avance significativo, aún enfrenta desafíos en su implementación efectiva, especialmente en lo que respecta a nuevas amenazas digitales como la difusión no consentida de imágenes o el uso de IA para crear contenido sin autorización. A diferencia de Argentina y Brasil, Ecuador todavía está en proceso de consolidar su legislación para enfrentar estos desafíos tecnológicos emergentes.

En resumen, mientras que Argentina y Brasil han avanzado en la actualización y aplicación de sus leyes de protección de datos personales para enfrentar desafíos digitales, Ecuador se encuentra en una etapa de desarrollo y adaptación de su marco legal para abordar eficazmente las nuevas amenazas en el ámbito de la privacidad y la seguridad digital.

2.2.2.1 Sentencias judiciales relevantes en casos de extorsión por difusión de imágenes.

La extorsión a través de la difusión de imágenes generadas por inteligencia artificial (IA) representa un desafío significativo para el derecho penal contemporáneo. Los avances tecnológicos han facilitado la creación de contenido digital que puede emplearse para amenazar y extorsionar a individuos, lo que plantea interrogantes sobre la eficacia de las legislaciones actuales. Este fenómeno es objeto de análisis en diversas jurisdicciones, incluyendo Ecuador, donde se están evaluando comparativamente las sentencias judiciales para fortalecer la legislación y las prácticas judiciales.

El artículo 185 del Código Orgánico Integral Penal (COIP) de Ecuador establece sanciones de prisión para quienes obtengan beneficios económicos o de otra índole mediante amenazas. Aunque esta normativa aborda la extorsión en términos generales,

no contempla explícitamente las amenazas digitales, como aquellas que implican la creación y difusión de imágenes alteradas por IA. La rápida evolución de la tecnología digital ha superado en muchos casos la capacidad de adaptación de las leyes, permitiendo que los delincuentes exploten lagunas legales sin temor a una persecución efectiva.

En Ecuador, se han documentado casos donde cibercriminales utilizan tecnología

de deepfake y vulneran cuentas de redes sociales para llevar a cabo estafas, incluyendo la clonación de voces con IA para cometer extorsiones. Estos incidentes afectan gravemente la privacidad y los derechos fundamentales de las personas, resaltando la necesidad urgente de ajustar la legislación para abordar estos nuevos riesgos.

Aunque Ecuador ha avanzado en la tipificación de delitos relacionados con la pornografía infantil, aún enfrenta desafíos para abordar específicamente los casos de deepfakes. La rápida evolución de la IA exige actualizaciones legales constantes para enfrentar adecuadamente estos nuevos delitos. Es esencial que las autoridades ecuatorianas fortalezcan su marco normativo, implementen medidas preventivas y promuevan la educación sobre el uso responsable de la tecnología, garantizando así la protección de los derechos de las víctimas y la integridad social.

Para enfrentar este desafío, Ecuador podría considerar la adaptación de sus leyes a los desarrollos tecnológicos, tomando como referencias normativas internacionales que abordan de manera más directa estos delitos. Por ejemplo, en marzo de 2025, España aprobó una reforma del Código Penal que incluye la penalización de los deepfakes y el grooming, buscando proteger a los menores de las amenazas digitales. Incorporar explícitamente la creación y difusión de imágenes manipuladas por IA en la legislación penal ecuatoriana permitiría que las amenazas digitales sean reconocidas como delitos y, por ende, puedan ser perseguidas judicialmente de manera más efectiva.

La inclusión de medidas de protección más estrictas en cuanto a la privacidad y el derecho a la imagen personal también sería un paso importante para mejorar la legislación. Las personas deben tener garantizado su derecho a que su imagen no sea utilizada sin su consentimiento en contextos que puedan dañar su integridad o honor. La legislación ecuatoriana podría adaptarse a este nuevo escenario, incorporando normas que protejan a los ciudadanos de los daños causados por la difusión de contenido manipulado digitalmente.

La adaptación de las leyes a los avances tecnológicos no solo mejoraría la efectividad del sistema de justicia, sino que también fortalecería la protección de los derechos de las personas en el entorno digital. La extorsión mediante la difusión de imágenes generadas por IA es un fenómeno en aumento, y Ecuador necesita estar preparado para enfrentar estos delitos de manera adecuada, garantizando que su legislación esté al día con las tecnologías emergentes que modifican el panorama de la

delincuencia. La actualización del marco legal es fundamental para brindar una respuesta adecuada a los nuevos retos que surgen con el avance de la tecnología y proteger a los ciudadanos de la amenaza que representa la extorsión digital.

Análisis de casos de extorsión nacionales

En Ecuador, los casos de extorsión digital han ido en aumento, reflejando la compleja interacción entre la tecnología y el crimen. Aunque las estadísticas oficiales pueden variar, se han documentado múltiples incidentes que destacan la gravedad de esta problemática.

Caso 1: Extorsión mediante imágenes íntimas (2024)

En enero de 2025, se conoció el caso de Jean Carlos B. y Juan Carlos B., quienes fueron sentenciados a seis años y ocho meses de prisión por extorsionar a un hombre. Estos individuos grabaron sin consentimiento videos de contenido sexual de la víctima y, bajo la amenaza de difundirlas, exigieron pagos que ascendieron a 5.000 dólares.

Caso 2: "Vacuna" en el sector comercial (2024)

En mayo de 2024, se desarticuló una red delictiva que operaba bajo la modalidad de "vacuna". Esta organización exigía pagos semanales o mensuales a comerciantes y taxistas a cambio de brindarles "seguridad". La banda utilizaba amenazas directas y, en algunos casos, atentados físicos contra negocios y vehículos de las víctimas.

Caso 3: Extorsión familiar (2024)

En abril de 2024, se descubrió una red de extorsión que operaba desde el seno familiar. Un ciudadano fue víctima de chantaje por parte de su propia hermana y cuñado, quienes, junto con otros cómplices, exigían 10.000 dólares a cambio de no atentar contra su integridad. La investigación reveló que la información sobre la víctima era proporcionada por miembros de su propia familia.

Caso 4: Extorsión con amenazas de difusión de contenido íntimo (2024)

En septiembre de 2024, una mujer fue víctima de extorsión cuando recibió

amenazas de difusión de contenido íntimo. Los extorsionadores exigieron 1.000 dólares a cambio de no atentar contra su vida o la de su familia. La investigación llevó a la aprehensión de tres personas involucradas en el delito.

2.2.2.2 Legislación latinoamericana comparada con Ecuador sobre responsabilidad en casos similares de extorsión por difusión de imágenes generadas por la I.A.

El uso creciente de la inteligencia artificial (IA) para la creación de imágenes plantea desafíos legales significativos en el ámbito del derecho penal, especialmente en casos de extorsión y difusión no autorizada de contenido visual. Es esencial analizar cómo diferentes países han legislado respecto a la responsabilidad legal en estos contextos, enfocándonos en las legislaciones de Argentina y Brasil, y estableciendo comparaciones con la de Ecuador.

Argentina

En Argentina, la Ley 25.326 de Protección de Datos Personales y el Código Penal conforman el marco principal para la protección de datos y la sanción de la extorsión digital.

Ley 25.326: Regula la recopilación, almacenamiento y difusión de datos personales, estableciendo sanciones para su uso indebido. Esta ley garantiza el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre ellas se registre.

Código Penal: Sanciona la extorsión como un delito grave, con penas que pueden incluir privación de libertad y multas significativas. La extorsión se define como cualquier amenaza empleada para obtener beneficios indebidos, destacando la gravedad de este delito en el ordenamiento jurídico argentino.

La legislación argentina destaca por su enfoque integral en la protección de datos personales y la sanción de delitos digitales, ofreciendo un marco robusto para enfrentar los desafíos que presenta la tecnología en el ámbito legal.

Brasil

En Brasil, la Ley General de Protección de Datos (LGPD) y el Código Penal constituyen el marco legal para la protección de datos y la sanción de la extorsión digital.

LGPD (2018): Regula el tratamiento de datos personales, estableciendo derechos y obligaciones tanto para individuos como para organizaciones. La ley exige el consentimiento libre e inequívoco del titular para el tratamiento de sus datos y crea la Autoridad Nacional de Protección de Datos (ANPD) para supervisar su cumplimiento.

Código Penal: Incluye disposiciones sobre extorsión y otros delitos relacionados con el uso indebido de datos personales, con penas que varían según la gravedad del delito. La ley establece sanciones administrativas por incumplimiento, como multas y suspensión de actividades, reforzando la protección contra abusos en línea.

La LGPD representa un avance significativo en el control de los datos personales en Brasil, imponiendo obligaciones estrictas a las entidades que manejan estos datos y sancionando su uso indebido.

Ecuador

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) también busca proteger los datos de los ciudadanos, pero su legislación está en una etapa de desarrollo comparada con la de Brasil. Aunque el Código Penal ecuatoriano sanciona la extorsión, no tiene un enfoque claro sobre delitos cibernéticos relacionados con los datos personales, lo que deja ciertos vacíos legales en el tratamiento de estos nuevos delitos digitales.

Comparando las legislaciones, Argentina y Brasil han avanzado significativamente en la creación de marcos legales específicos que abordan directamente los delitos digitales y la protección de datos personales. Ecuador, por su parte, está en proceso de fortalecer su

legislación en este aspecto, pudiendo beneficiarse de las experiencias y normativas implementadas en estos países para mejorar sus leyes relacionadas con la protección de datos y la extorsión digital.

2.2.2.3 Interpretación judicial de normativas existentes

El uso creciente de inteligencia artificial (IA) para la creación de imágenes ha introducido desafíos legales significativos, especialmente en casos de extorsión y difusión no autorizada de contenido visual. Tanto a nivel nacional como internacional, los tribunales están adaptando las legislaciones existentes para abordar estos delitos facilitados por la tecnología. A continuación, se analiza cómo se interpretan y aplican las leyes en estos casos, con ejemplos de Ecuador, Argentina y Brasil.

Interpretación Judicial en Ecuador

En Ecuador, el Código Orgánico Integral Penal (COIP) y la Ley de Protección de Datos Personales son fundamentales para abordar delitos cibernéticos como la extorsión. Un caso destacado en Quito en 2022 involucró la extorsión a una víctima mediante la amenaza de divulgar imágenes íntimas generadas por IA. El tribunal aplicó el artículo 185 del COIP, que sanciona la extorsión, adoptando una interpretación que abarca la naturaleza digital de los delitos modernos.

Interpretación Judicial en Argentina

En Argentina, la Ley 25.326 de Protección de Datos Personales y el Código Penal son esenciales en casos de extorsión digital. Un ejemplo significativo es el caso "Belén R." en 2018, donde se utilizó IA para generar imágenes falsas con fines de extorsión. La corte enfatizó que la ley protege contra cualquier uso no autorizado de datos personales, incluyendo imágenes digitales creadas por IA. Este fallo refleja el esfuerzo de Argentina por adaptar su marco legal a los avances tecnológicos y proteger la privacidad en el entorno digital.

Interpretación Judicial en Brasil

En Brasil, la Ley General de Protección de Datos (LGPD) y el Código Penal abordan la extorsión y la difusión no consentida de imágenes. El caso "João S." en 2021 es ilustrativo, donde se extorsionó a una víctima mediante imágenes generadas por IA. El Tribunal Superior de Justicia determinó que la LGPD protege contra el uso no autorizado de datos personales, incluyendo aquellos generados por IA, asegurando que las víctimas de extorsión digital reciban respaldo legal.

Comparativa y Reflexión

Al comparar las legislaciones de Ecuador, Argentina y Brasil, se observa que, aunque comparten la preocupación por la protección de datos personales, existen diferencias en el nivel de desarrollo y especificidad de sus normativas. Argentina y Brasil han implementado leyes detalladas que abordan explícitamente la extorsión digital y el uso de tecnologías emergentes como la IA. Ecuador, por su parte, está en proceso de fortalecer su legislación para enfrentar estos desafíos, adaptándose a las nuevas formas de violación de datos personales en el entorno digital.

2.2.3 UNIDAD III: Propuestas de Política y Regulación sobre la extorsión por imágenes generadas por la inteligencia artificial.

La inteligencia artificial (IA) ha transformado múltiples sectores, pero su uso indebido, especialmente en la creación y difusión de imágenes falsas, presenta desafíos significativos en términos de ciberseguridad y protección de datos personales. En Ecuador, es esencial adaptar las políticas y regulaciones para abordar eficazmente los casos de extorsión mediante la difusión de imágenes generadas por IA. A continuación, se presentan propuestas para fortalecer el marco jurídico y proteger a las víctimas de estos delitos.

Propuesta 1: Reforma del Código Orgánico Integral Penal (COIP)

Se propone actualizar el COIP para incluir delitos específicos relacionados con el uso de IA en la generación de imágenes comprometedoras. Aunque el COIP aborda delitos como la extorsión y la violación de la privacidad, no contempla explícitamente el uso de IA en estos contextos. La reforma sugerida establece sanciones más severas cuando se utilicen tecnologías avanzadas para difundir o amenazar con difundir contenido generado o manipulado por IA que afecte la intimidad y reputación de las personas.

Propuesta 2: Fortalecimiento de la Ley de Protección de Datos Personales

La Ley de Protección de Datos Personales de Ecuador, promulgada en 2021, debe revisarse para abarcar específicamente el tratamiento y la protección de datos generados por IA. Esto incluiría garantizar que el consentimiento del titular sea obligatorio para el uso de imágenes creadas o manipuladas por IA, reforzando la privacidad y seguridad de los ciudadanos en el entorno digital.

Propuesta 3: Creación de Unidades Especializadas en Delitos Cibernéticos

Es fundamental establecer unidades especializadas dentro de las fuerzas de seguridad y el sistema judicial para investigar y procesar delitos cibernéticos relacionados con la IA. Estas unidades, como la Unidad Nacional Especializada en Investigación de Ciberdelito de la Fiscalía General del Estado, permitirían una respuesta más rápida y eficaz a las denuncias de extorsión digital, mejorando la capacidad de las autoridades para rastrear y detener a los perpetradores.

Avances Actuales en Ecuador

Ecuador ha tomado medidas significativas en la lucha contra el cibercrimen. En noviembre de 2024, el país participó en la implementación del "Punto de Contacto 24/7", una red internacional que facilita la cooperación en la investigación de delitos informáticos. Además, en junio de 2022, se creó la Unidad Nacional Especializada en Investigación de Ciberdelito, encargada de investigar delitos como la revelación ilegal de bases de datos y ataques a la integridad de sistemas informáticos.

2.2.3.1 Efectividad de las medidas de prevención y protección existentes sobre la extorsión por imágenes generadas con I.A.

La creciente utilización de imágenes manipuladas mediante inteligencia artificial (IA) con fines de extorsión representa una amenaza emergente que desafía la protección de los derechos individuales y la seguridad cibernética. En Ecuador, es esencial evaluar y reforzar continuamente las estrategias de prevención y protección para hacer frente a estas amenazas tecnológicas. Este análisis se centra en la eficacia de las legislaciones vigentes, las políticas implementadas y las tácticas adoptadas para salvaguardar a las víctimas de la extorsión digital.

La extorsión mediante la difusión de imágenes generadas por IA es un fenómeno en ascenso, donde los delincuentes emplean tecnologías avanzadas, como los deepfakes, para crear contenido visual comprometedor de una persona con el propósito de extorsionarla. Este tipo de extorsión ocurre cuando los agresores producen imágenes o videos falsificados que muestran a la víctima en situaciones comprometedoras y luego amenazan con difundir este material a cambio de dinero o favores. Las imágenes manipuladas, que pueden parecer auténticas, se utilizan como herramientas poderosas para intimidar a las víctimas y obtener beneficios ilícitos. La creación de estos contenidos es facilitada por herramientas avanzadas de IA que permiten una manipulación sofisticada de imágenes y videos.

En cuanto a las medidas para prevenir y proteger a las personas contra este tipo de delitos, existen iniciativas tanto legales como tecnológicas, aunque persisten desafíos significativos. En Ecuador, la legislación penal, a través del Código Orgánico Integral Penal (COIP), tipifica ciertos delitos relacionados con la extorsión y otros crímenes cibernéticos. Sin embargo, aún no aborda específicamente las amenazas derivadas de

imágenes generadas por IA. Además, la Ley Orgánica de Protección de Datos Personales tiene implicaciones para salvaguardar la privacidad y el derecho a la imagen personal, aspectos relevantes en este contexto, ya que estas leyes buscan garantizar que las personas mantengan el control sobre el uso de sus imágenes en línea.

A nivel tecnológico, existen herramientas de detección de deepfakes, como Reality Defender, Deepware Scanner y Microsoft Video Authenticator, que son capaces de identificar contenido manipulado mediante IA. Estas herramientas ayudan a verificar la autenticidad de imágenes y videos en línea, lo que puede ser útil tanto para las víctimas de extorsión como para las plataformas que buscan prevenir la difusión de contenido falso. Además, herramientas de verificación como InVID permiten a los usuarios analizar y autenticar el contenido visual, contribuyendo a reducir el impacto de las imágenes generadas por IA que podrían ser utilizadas con fines maliciosos.

No obstante, a pesar de los avances tecnológicos y las medidas legales existentes, la eficacia de estas estrategias sigue siendo limitada. Las leyes, en muchos casos, no están suficientemente adaptadas para enfrentar la amenaza de los deepfakes, lo que genera un vacío legal que dificulta el procesamiento adecuado de los delitos relacionados con el uso de IA. Además, la rapidez con que evolucionan las tecnologías de manipulación digital hace que las herramientas de detección no siempre sean suficientes, ya que las técnicas de creación de deepfakes se vuelven cada vez más sofisticadas y difíciles de identificar. Otro desafío importante es la accesibilidad de estas tecnologías, ya que muchas de las herramientas de detección y verificación no son de fácil acceso para el público general, limitando su efectividad en la protección de las víctimas.

Además, el uso de imágenes generadas por IA plantea desafíos sociales y psicológicos. La difusión de contenido falso puede generar desconfianza generalizada, afectando la percepción de la realidad y dificultando la identificación de contenido auténtico. Las víctimas de extorsión pueden experimentar consecuencias psicológicas graves, como miedo, vergüenza o ansiedad, lo que complica la denuncia de estos crímenes o la búsqueda de ayuda.

Para mejorar las medidas de prevención y protección contra la extorsión por imágenes generadas con IA, es necesario actualizar las leyes para abordar específicamente los delitos relacionados con el uso de esta tecnología. Es crucial que las

normativas legales se adapten para incluir las amenazas emergentes que surgen con el uso de IA en el ámbito digital. Asimismo, invertir en tecnologías de detección más precisas y accesibles puede jugar un papel fundamental en la protección de las personas. Finalmente, promover la educación digital, enfocándose en la protección de la privacidad y el reconocimiento de contenido manipulado, es esencial para crear una cultura de seguridad en línea y reducir el impacto de estos delitos.

2.2.3.2 La Responsabilidad de los Actores Institucionales y Sociales en la Regulación de la Extorsión Cibernética por Imágenes Manipuladas con IA.

La extorsión a través de la difusión de imágenes manipuladas con inteligencia artificial (IA) representa una amenaza creciente que afecta la privacidad y seguridad de las personas. En Ecuador, este fenómeno ha ganado relevancia, evidenciando la necesidad de una respuesta coordinada entre el gobierno, la industria tecnológica y la sociedad civil.

Responsabilidad del Gobierno

Las autoridades gubernamentales tienen la misión de establecer un marco legal robusto que aborde los delitos cibernéticos, incluyendo la extorsión mediante imágenes generadas por IA. En noviembre de 2024, Ecuador ratificó su adhesión al Convenio de Budapest, reforzando su compromiso en la lucha contra el cibercrimen y promoviendo la cooperación internacional en investigaciones relacionadas con delitos informáticos.

Papel de la Industria Tecnológica

Las empresas tecnológicas deben ser proactivas en el desarrollo de soluciones que prevengan el uso indebido de sus plataformas. La implementación de herramientas de detección y prevención de contenido manipulado con IA es esencial. Por ejemplo, en agosto de 2023, se reportó que cibercriminales en Ecuador utilizaban tecnología 'deepfake' para realizar estafas relacionadas con criptomonedas, vulnerando cuentas de redes sociales.

Rol de la Sociedad Civil

La sociedad civil, incluyendo organizaciones no gubernamentales y ciudadanos, juega un papel crucial en la vigilancia y promoción de políticas efectivas. En octubre de

2023, se denunció un caso en Quito donde estudiantes fueron víctimas de violencia sexual digital mediante el uso de IA, lo que llevó a la Fiscalía a abrir una investigación. Además, la educación y concienciación sobre los riesgos asociados con la tecnología y la ciberseguridad son fundamentales para empoderar a las personas y reducir la incidencia de estos delitos.

La colaboración entre estos actores es esencial para desarrollar y aplicar políticas y regulaciones efectivas que protejan a las víctimas y sancionen a los perpetradores de delitos cibernéticos. La rápida evolución de la tecnología requiere una adaptación constante de las estrategias y herramientas utilizadas para combatir estos delitos.

Abvocacy y lobbying, defensa e incidencia legal en la responsabilidad jurídica frente a casos de extorsión por difusión de imágenes generadas mediante I.A.

En el ámbito legal, los términos "advocacy" y "lobbying" son fundamentales para impulsar cambios legislativos y proteger derechos específicos. Mientras que el "advocacy" se refiere a la promoción y defensa de una causa, buscando influir en las decisiones públicas a través de la educación y sensibilización de la sociedad, el "lobbying" implica acciones más directas, como interactuar con legisladores y funcionarios gubernamentales para influir en la creación o modificación de leyes específicas.

En el contexto de la extorsión mediante la difusión de imágenes generadas por inteligencia artificial (IA), tanto el "advocacy" como el "lobbying" desempeñan roles cruciales. Estas estrategias permiten visibilizar los riesgos asociados con el uso malintencionado de la IA, promover la implementación de normativas que salvaguarden a las víctimas y fortalecer el marco legal para abordar los desafíos éticos y jurídicos que surgen con los avances tecnológicos.

Las organizaciones no gubernamentales (ONG) y los grupos defensores de derechos deben involucrarse activamente en la formulación de políticas públicas. Su participación puede incluir la recopilación de datos, realización de campañas de sensibilización y presentación de propuestas legislativas que aborden específicamente la problemática de la extorsión digital mediante IA. Estas acciones contribuyen a la creación de un entorno legal más robusto y adaptado a las nuevas amenazas tecnológicas.

Por ejemplo, el "lobbying" puede ser una herramienta efectiva para influir en los

legisladores y asegurar que se adopten políticas que realmente protejan a las víctimas de extorsión digital.

2.2.3.3 Garantías para la protección de Derechos individuales y la promoción de la responsabilidad corporativa en el uso de la IA.

La inteligencia artificial (IA) ha progresado a un ritmo acelerado, brindando numerosos beneficios, pero también presentando nuevos retos en relación con los derechos individuales y la responsabilidad empresarial. En Ecuador, resulta esencial ajustar el marco legal para salvaguardar a los ciudadanos y fomentar la responsabilidad de las empresas en el uso de la IA, especialmente en casos de extorsión mediante la difusión de imágenes generadas por esta tecnología. A continuación, se presentan diversas propuestas de políticas y regulaciones orientadas a alcanzar estos objetivos.

Protección de Derechos Individuales

La protección de los derechos individuales en el ámbito de la IA exige la actualización de las leyes vigentes, la implementación de nuevas regulaciones y el fortalecimiento de la educación y concienciación sobre los riesgos asociados con la IA.

- Actualización de la Legislación Vigente: Es necesario revisar las leyes actuales en Ecuador, como el Código Orgánico Integral Penal (COIP) y la Ley de Protección de Datos Personales, para abordar específicamente los desafíos que presenta la IA.
- Consentimiento Informado: Se debe reforzar el principio del consentimiento informado en la Ley de Protección de Datos Personales, garantizando que los datos personales, incluidas las imágenes generadas por IA, no se utilicen sin el consentimiento explícito de la persona.
- Derecho al Olvido: Implementar el derecho al olvido permitiría a las personas solicitar la eliminación de sus datos personales de las plataformas digitales, protegiendo su privacidad y dignidad en la era digital.

Promoción de la Responsabilidad Corporativa

Las empresas que desarrollan y utilizan tecnologías de IA deben asumir una

responsabilidad significativa en la protección de los derechos de los usuarios y en la prevención de abusos. Esto se puede lograr mediante políticas corporativas sólidas, auditorías regulares y el cumplimiento de estándares éticos y legales.

- Políticas Corporativas y Códigos de Conducta: Las empresas deben establecer políticas claras y códigos de conducta que regulen el uso de la IA de manera ética y responsable, incluyendo la prohibición de generar contenido sin el consentimiento de los individuos afectados.
- Auditorías y Evaluaciones de Impacto: Es fundamental que las empresas realicen auditorías regulares y evaluaciones de impacto para identificar y mitigar los riesgos asociados con el uso de la IA, permitiendo la implementación de medidas preventivas adecuadas.
- Transparencia y Rendición de Cuentas: La transparencia en las prácticas corporativas y la disposición a rendir cuentas son esenciales para construir confianza y asegurar el cumplimiento ético y legal en el uso de la IA.

Educación y Concienciación

La educación y la concienciación son fundamentales para proteger los derechos individuales y promover la responsabilidad corporativa en el uso de la IA. Esto implica educar tanto al público general como a los profesionales del derecho y la tecnología sobre los riesgos y las mejores prácticas relacionadas con la IA.

- Programas de Educación Pública: Implementar programas de educación pública para informar a los ciudadanos sobre los riesgos asociados con la IA y cómo proteger sus derechos es fundamental para empoderar a los individuos y ayudarlos a mitigar los riesgos asociados con la IA.
- Capacitación Profesional Continua: Los profesionales del derecho y la tecnología deben recibir capacitación continua sobre las últimas tendencias y desafíos en el uso de la IA, asegurando que estén bien equipados para enfrentar los desafíos legales y éticos asociados con la IA.
- Campañas de Concienciación Corporativa: Las corporaciones deben llevar a cabo campañas internas de concienciación para educar a sus empleados sobre el uso ético y responsable de la IA, inculcando una cultura de responsabilidad y ética en el uso de tecnologías avanzadas.

Cooperación Internacional

La cooperación internacional es vital para abordar los desafíos transnacionales asociados con la IA y la extorsión digital. Ecuador debe fortalecer su colaboración con organismos internacionales y participar activamente en la elaboración de estándares y regulaciones globales.

- Adhesión a Tratados Internacionales: Ecuador debe adherirse a tratados internacionales como el Convenio de Budapest sobre Cibercriminalidad, que promueve la cooperación internacional en la lucha contra los delitos cibernéticos, proporcionando un marco legal robusto para la cooperación en la lucha contra los delitos cibernéticos, incluyendo la extorsión digital.
- Colaboración con Organismos Internacionales: La colaboración con organismos internacionales, como la INTERPOL y la Organización de Estados Americanos (OEA), es crucial para enfrentar la naturaleza transnacional de muchos delitos cibernéticos, permitiendo compartir conocimientos, recursos y mejores prácticas en la lucha contra los delitos cibernéticos.

Desarrollo de Tecnología de Protección

El desarrollo y la implementación de tecnologías avanzadas para la protección de datos personales y la prevención de la extorsión digital son estrategias cruciales. Estas tecnologías pueden incluir herramientas de detección de imágenes manipuladas y sistemas de alerta temprana.

- Herramientas de Detección de Imágenes Manipuladas: Invertir en el desarrollo de herramientas avanzadas para detectar imágenes manipuladas por IA puede ayudar a prevenir la extorsión digital, identificando y mitigando el uso indebido de contenido generado por IA.
- Sistemas de Alerta Temprana: Implementar sistemas de alerta temprana puede ayudar a identificar actividades sospechosas y prevenir la difusión de contenido no autorizado, detectando y respondiendo rápidamente a amenazas cibernéticas y protegiendo a los usuarios y sus datos personales.

CAPÍTULO III. METODOLOGÍA

Con este propósito, en el presente estudio denominado “La responsabilidad legal en casos de extorsión por difusión de imágenes generadas por inteligencia artificial” se emplearon varios métodos, técnicas, instrumentos y recursos que permitieron alcanzar los objetivos planteados.

3.1 Unidad de análisis

La investigación se centró en el marco legal ecuatoriano, específicamente en las disposiciones relacionadas con la responsabilidad legal en casos de extorsión por difusión de imágenes generadas por IA. Se analizaron las leyes y regulaciones pertinentes que abordan este fenómeno emergente, considerando cualquier disposición relacionada con la difusión no autorizada, el uso indebido o la manipulación maliciosa de imágenes generadas por IA. El objetivo fue comprender cómo estas disposiciones legales afectan la atribución de responsabilidad y la protección de las víctimas en este contexto específico de extorsión cibernética por difusión de imágenes sexuales.

3.2 Métodos

Para estudiar el problema se emplearon los siguientes métodos:

Método dogmático-jurídico: El método dogmático-jurídico se aplica realizando un análisis y síntesis de las normas legales relacionadas con la extorsión y la I. A. en Ecuador. Se analizarán los conceptos y principios jurídicos para interpretar claramente las reglas legales pertinentes dentro del Derecho positivo ecuatoriano, específicamente en lo que respecta a la responsabilidad legal por el uso indebido de imágenes generadas por IA. Wart,

G. (1980).

Método jurídico descriptivo: Este método implicará una descomposición detallada del fenómeno de la extorsión mediante imágenes generadas por IA en sus componentes más básicos. Se preservará una delimitación precisa del tema para obtener una visión completa y detallada del fenómeno en el contexto de la legislación ecuatoriana. Rivera Waleska, J. (2007).

Método de comparación jurídica: Se utilizará el método de comparación jurídica para comparar las disposiciones legales ecuatorianas sobre la responsabilidad en casos de extorsión por imágenes generadas por IA con las normativas de otros países. Esto ayudará

a identificar similitudes, diferencias y avances de mejora potencial. Morineau, P. (2016).

Método exegético: El método exegético será instrumental para interpretar las leyes ecuatorianas relevantes. Se procederá mediante el análisis del sentido de las palabras en las normas legales, utilizando la lógica y considerando la intención del legislador al promulgar dichas leyes. Melián Vega, A. (2011).

3.3 Tipo de Investigación

Investigación jurídica descriptiva: Para el tema de la responsabilidad legal en casos de extorsión por difusión de imágenes generadas por IA, se aplicó una investigación jurídica descriptiva. Esto implicó utilizar el método analítico de manera pura para descomponer el problema en sus diversos aspectos y establecer relaciones y niveles que ofrecieran una comprensión profunda del funcionamiento de las normas legales involucradas. Este enfoque permitió una comprensión detallada de las disposiciones legales aplicables y su aplicación en situaciones específicas de extorsión con imágenes generadas por IA.

Investigación exploratoria: Según Gómez y López (2020), "las investigaciones exploratorias se realizan generalmente cuando se busca examinar un tema con poca atención previa o que no se ha abordado anteriormente en profundidad" (p. 39). Por eso, se realizó una investigación exploratoria, ya que permitió identificar diversas perspectivas, evaluar la viabilidad práctica y legal y anticipar posibles desafíos sobre la responsabilidad legal en casos de extorsión por difusión de imágenes generadas por IA.

Investigación dogmática: De acuerdo con García (2018), "un estudio normativo o dogmático implica la descripción, análisis, interpretación y aplicación de normas jurídicas, junto con la elaboración de conceptos y métodos para construir un ordenamiento dinámico y establecer instituciones legales" (p. 5). En este sentido, la investigación jurídica dogmática permitió analizar la normativa legal y principios jurídicos esenciales para entender cómo se ajustan las leyes existentes a la extorsión por difusión de imágenes generadas por IA y los ajustes normativos necesarios.

Investigación jurídica descriptiva: Según Ramírez y Pérez (2019), "las investigaciones descriptivas tienen como objetivo identificar y detallar las características más significativas de grupos, individuos, comunidades, conceptos u otros fenómenos sujetos a análisis" (p. 43). Este tipo de investigación posibilitó obtener una visualización detallada de cómo se está abordando la responsabilidad legal en casos de extorsión por

difusión de imágenes generadas por IA en diferentes jurisdicciones y sectores a nivel mundial, así como observar el impacto de dicha implementación.

3.4 Diseño de Investigación

Dado lo complejo de la investigación y los objetivos que se buscaban alcanzar, se optó por un diseño no experimental. En este tipo de diseño, fue crucial utilizar el software ATLAS.ti, una herramienta especializada en el análisis de datos cualitativos. ATLAS.ti nos ayudó a manejar y examinar la información de manera más eficiente.

Utilizamos el software para analizar las entrevistas, codificando y clasificando los datos de acuerdo con los criterios establecidos para el estudio. Este proceso detallado nos permitió interpretar la información de manera precisa y cumplir con los objetivos de nuestra investigación de manera efectiva.

3.5 Población y muestra

3.5.1 Población

La población implicada en la presente investigación está comprendida por Abogados penalistas y conocedores informáticos en inteligencia artificial realizado en la provincia de Chimborazo, cantón Riobamba.

3.5.2 Muestra

Al ser la población infinita, es decir, no se conoce con exactitud la cantidad a saber, la muestra del presente estudio estuvo constituida por (2) dos abogados penalistas y (2) conocedores informáticos en inteligencia artificial, haciendo uso del criterio de elección de forma intencional, no probabilístico y por conveniencia, en base a los siguientes criterios y exclusión:

- Abogados que hayan obtenido un título de tercer nivel en Derecho e informáticos que hayan obtenido un título de tercer nivel.
- Que laboren en libre ejercicio profesional.
- Posean una Maestría o Especialidad en Derecho Penal, posean una Maestría o Especialidad en Inteligencia Artificial
- Cuenten con conocimientos elementales en Inteligencia Artificial.

3.6 Técnicas e instrumentos de investigación

En el presente trabajo investigativo se usó como técnica la entrevista y como instrumento la guía de entrevista.

3.6.1 Técnica para el tratamiento de la información.

En esta investigación se utilizarán:

- Técnica: Observación, Entrevista.
- Instrumento: Guía de entrevista.

3.6.2 Instrumento de investigación

Para aplicar la técnica de investigación, es necesario como instrumento una guía de entrevista aplicada a la población involucrada en el trabajo investigativo.

3.7 Técnicas para el tratamiento de información

1. Elaboración del instrumento de investigación.
2. Aplicación del instrumento de investigación.
3. Resumen de las entrevistas.
4. Procesamiento de los datos e información, a través del software ATLAS. Ti.
5. Interpretación y análisis de resultados mediate la aplicación ATLAS. Ti, que permitió la creación de códigos y criterios que hayan tenido concurrencia y sean adheridos a nuestros objetivos de investigación, para su posterior interpretación mediante una red semántica debidamente explicada.
6. Discusión de los resultados.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1 Resultados

4.1.1 Fundamentos teóricos y legales relacionados con la extorsión y el uso de imágenes generadas por la I.A.

La figura 1 presenta un mapa mental que ilustra la compleja interacción entre la Inteligencia Artificial (IA) y la extorsión, enfocándose en cómo las imágenes generadas por IA pueden ser utilizadas como herramientas de extorsión. Este diagrama se divide en dos clústeres principales que están interconectados mediante diversas relaciones y dependencias.

Clúster 1: Inteligencia Artificial

Aspecto Técnico: Se detallan las técnicas de IA, como las Redes Generativas Adversarias (GANs) y las Redes Neuronales, que son fundamentales en la creación de imágenes sintéticas. Estas técnicas producen contenidos como deepfakes y otras formas de síntesis de imágenes, los cuales requieren sistemas de validación y detección para verificar su autenticidad.

Impacto: Se abordan los riesgos asociados, como la suplantación y manipulación de identidad, así como las medidas preventivas necesarias, que incluyen educación y sistemas de detección.

Clúster 2: Extorsión

Legal: Se analizan las legislaciones nacionales, como el Código Orgánico Integral Penal (COIP) Art. 185 y las leyes de protección de datos, junto con las legislaciones internacionales, incluyendo el Reglamento General de Protección de Datos (GDPR) y el Convenio de Budapest.

Jurisprudencia: Se revisan casos nacionales que establecen precedentes importantes en la materia.

Responsabilidad:

Corporativa: Implica medidas de prevención y auditorías.

Individual: Aborda los deberes y la privacidad de las personas.

Interconexiones Clave:

Las técnicas de IA facilitan la creación de contenido que puede ser utilizado para extorsionar, lo cual es regulado por las legislaciones nacionales y genera precedentes en los casos judiciales.

La validación técnica asegura la autenticidad del contenido, mientras que los riesgos identificados determinan las responsabilidades individuales.

La prevención implementa mecanismos de protección, y los casos internacionales ofrecen interpretaciones que guían la jurisprudencia.

Estas interrelaciones demuestran cómo la tecnología de IA, aunque neutral en su naturaleza, puede ser empleada con fines maliciosos como la extorsión. Esto requiere una respuesta coordinada desde los ámbitos técnico, legal y social. El marco regulatorio y las responsabilidades establecidas buscan prevenir y mitigar estos riesgos, mientras que los mecanismos de validación y control técnico apoyan la implementación de estas protecciones.

La estructura del mapa mental enfatiza la naturaleza multidisciplinaria del problema, donde las soluciones técnicas deben trabajar en conjunto con los marcos legales y las responsabilidades tanto corporativas como individuales para abordar efectivamente la problemática de la extorsión mediante imágenes generadas por IA.

Desafíos Legales en Ecuador:

En Ecuador, la legislación sobre protección de datos, como la Ley Orgánica de Protección de Datos Personales, se centra en la recolección y manejo de datos personales. Sin embargo, la creación de imágenes falsas a través de IA plantea nuevos desafíos que estas leyes no abordan plenamente, como el uso no consensuado de la identidad visual de una persona.

Las leyes tradicionales de extorsión, tipificadas en códigos penales como actos de coacción para obtener beneficios económicos, no contemplan explícitamente el uso de herramientas tecnológicas avanzadas como la IA. Esto crea una brecha legal que puede ser explotada por los perpetradores de delitos cibernéticos.

Casos Relevantes:

En septiembre de 2023, el Instituto Nacional de Ciberseguridad (INCIBE) reportó un caso donde un adolescente fue víctima de sextorsión mediante un montaje fotográfico realizado con IA. El delincuente manipuló imágenes del menor para crear contenido explícito y luego lo extorsionó, exigiendo dinero a cambio de no difundir las imágenes.

En octubre de 2024, se informó sobre delincuentes que manipularon imágenes de migrantes utilizando IA para extorsionar a sus familiares. Estas personas crearon videos y fotos falsas de migrantes y las utilizaron para exigir pagos a sus seres queridos.

4.1.2 Influencia del uso de imágenes generadas con inteligencia artificial relacionadas con el delito de extorsión en el Ecuador con el fin de identificar áreas de mejora en la legislación.

La creciente utilización de imágenes generadas por inteligencia artificial (IA) con fines extorsivos plantea desafíos significativos para el sistema legal en Ecuador. La capacidad de crear contenido visual falso de alta fidelidad permite a los delincuentes amenazar a las personas con la difusión de material manipulado que puede dañar gravemente su reputación. Aunque este fenómeno es reconocido globalmente, en el contexto ecuatoriano aún no existe una regulación específica que aborde estos delitos, lo que genera un vacío legal que dificulta la protección efectiva de las víctimas.

El Código Orgánico Integral Penal (COIP) de Ecuador, en su artículo 185, establece sanciones para quienes obtienen beneficios mediante amenazas. Sin embargo, esta disposición no contempla las amenazas basadas en la manipulación digital de imágenes,

dejando fuera de la regulación los delitos cometidos con tecnologías emergentes como la IA. Esta laguna legislativa requiere una actualización que incluya los riesgos asociados a las amenazas digitales, especialmente aquellas derivadas del uso malintencionado de herramientas tecnológicas avanzadas.

Es fundamental que Ecuador desarrolle un marco legal que reconozca específicamente los delitos relacionados con la manipulación de imágenes y otros contenidos generados por IA. Esta tecnología ha sido empleada para extorsionar a personas mediante la creación de material falso que, de difundirse, puede tener consecuencias devastadoras en la vida de la víctima. La legislación debería incorporar

sanciones claras para quienes utilicen la IA con fines de extorsión, así como establecer mecanismos de protección para las personas afectadas por la difusión no autorizada de imágenes manipuladas.

Una de las áreas que requiere atención es la definición precisa de los delitos que implican la manipulación digital de imágenes generadas por IA. La inclusión de sanciones específicas para estos delitos permitiría al sistema judicial contar con las herramientas necesarias para procesar a los responsables de crear y difundir contenido falso con fines extorsivos. Además, es necesario fortalecer la protección de los derechos a la imagen y la privacidad, ampliando las leyes que regulan la difusión de imágenes no autorizadas, especialmente aquellas que causan daño a la reputación de las personas.

Otra área crucial es la responsabilidad de las plataformas digitales. Las redes sociales y otros sitios web suelen ser canales para la difusión de contenido manipulado. Por ello, es esencial regular la responsabilidad de estas plataformas en la detección, eliminación y prevención de la circulación de imágenes generadas por IA que puedan ser utilizadas para extorsionar a las personas. Las plataformas deben colaborar con las autoridades para frenar este tipo de delitos y garantizar la seguridad en línea de los usuarios.

La investigación sobre los fundamentos teóricos y legales relacionados con la extorsión y el uso de imágenes generadas por IA en Ecuador ha revelado varios puntos preocupantes. En primer lugar, se observa un panorama legal desactualizado. Las leyes actuales intentan proteger la privacidad y los datos personales, pero no abordan el uso malintencionado de la IA para crear imágenes falsas, dejando a las víctimas potenciales sin una protección legal clara. Además, jueces y fiscales enfrentan dificultades al tratar de aplicar leyes diseñadas para el mundo físico a delitos que ocurren en el ámbito digital con tecnología avanzada.

Al analizar casos tanto en Ecuador como en otros países, se evidencia un aumento en el uso de imágenes generadas por IA para chantajear a personas, y las respuestas legales han sido inconsistentes. Muchos delincuentes evaden las sanciones debido a que las leyes no contemplan específicamente estos nuevos métodos de extorsión. Expertos en derecho digital y ciberseguridad coinciden en que es urgente actualizar las leyes para incluir disposiciones específicas sobre la creación y uso de imágenes falsas generadas por IA.

Al comparar la situación de Ecuador con la de países como España y México, se observa que estos han implementado leyes que abordan directamente el uso malicioso de la IA. Ecuador podría aprender de sus experiencias, adoptando políticas efectivas como la educación pública sobre los riesgos de la manipulación de imágenes y la cooperación internacional entre agencias de justicia. Se recomienda revisar el Código Penal ecuatoriano para incluir delitos específicos relacionados con la creación y uso de imágenes generadas por IA para extorsión, definiendo claramente estos actos y estableciendo sanciones adecuadas. Además, es esencial fortalecer la Ley Orgánica de Protección de Datos Personales para abordar específicamente la manipulación digital de imágenes, garantizando que las víctimas tengan recursos legales claros y efectivos.

La educación también juega un papel fundamental. Es crucial formar tanto a profesionales legales como al público en general sobre los riesgos y señales de alerta relacionadas con la extorsión mediante imágenes generadas por IA. Esto incluye la capacitación de jueces, fiscales y abogados en nuevas tecnologías y sus implicaciones legales. Dado el carácter global de internet y la naturaleza transfronteriza de estos delitos, es necesaria una mayor cooperación internacional. Esto podría incluir acuerdos de colaboración para la investigación y el enjuiciamiento de casos, así como la armonización de leyes para facilitar la persecución de estos delitos a nivel global.

Actualmente, las leyes en Ecuador no abordan de manera específica la creación y uso de imágenes falsas generadas por IA para fines extorsivos. Aunque existen protecciones generales para la privacidad y los datos personales, estas no cubren explícitamente la manipulación digital de imágenes, lo que deja a las víctimas vulnerables y a los perpetradores sin sanciones claras. Los casos que involucran imágenes generadas por IA presentan complejidades únicas para el sistema judicial. La falta de claridad en la legislación dificulta encuadrar estos casos en las categorías tradicionales de extorsión y chantaje, especialmente cuando las imágenes, aunque no sean reales, pueden dañar significativamente la reputación y el bienestar emocional de las víctimas.

Al revisar casos en Ecuador y otros países, se observa un aumento en el uso de tecnología IA para crear contenido incriminatorio o comprometedor. Estos casos muestran cómo la tecnología puede ser utilizada para coaccionar y manipular a las personas. Comparando con países como España y México, se encuentra que estos tienen

marcos legales más avanzados que podrían servir de referencia. Algunos de estos países han comenzado a implementar leyes específicas para abordar

4.1.3 Tipos de extorsión vinculados a la difusión de imágenes sexuales generadas por la I.A.

4.1.3.1 Entrevista a Abogados Penalistas y conocedores informáticos en inteligencia artificial.

La recopilación de entrevistas realizadas a abogados penalistas y expertos en inteligencia artificial (IA) ofrece una visión profunda de la intersección entre el derecho y la tecnología, especialmente en casos de extorsión mediante imágenes falsas generadas por IA. Estas conversaciones destacan los desafíos legales, éticos y técnicos que surgen cuando la tecnología se utiliza con fines malintencionados. A continuación, se presentan resúmenes de las entrevistas realizadas:

Tabla 1. Entrevista 1

Nombre: Abg. Paul Pérez Resumen de la entrevista:

En la conversación con el abogado penalista Paul Pérez, se abordaron los desafíos legales relacionados con la extorsión mediante imágenes generadas por IA. Pérez señaló que, aunque Ecuador cuenta con leyes que tratan el chantaje y la privacidad, estas no están preparadas para enfrentar las complejidades de las nuevas tecnologías. La falta de claridad

legislativa sobre el manejo de imágenes creadas artificialmente dificulta la tarea de responsabilizar a los delincuentes y de imponer sanciones adecuadas. Destacó la necesidad de actualizar las leyes para incluir definiciones claras sobre estos delitos tecnológicos y enfatizó la importancia de capacitar a jueces y fiscales en estos temas. Asimismo, resaltó la relevancia de la cooperación internacional, ya que muchos de estos delitos trascienden fronteras. Pérez sugirió que un enfoque legislativo más flexible y adaptado a los avances tecnológicos es esencial para proteger eficazmente a las víctimas y garantizar que los responsables enfrenten las consecuencias correspondientes.

Autor: Karla Pacheco

Tapia Fuente: Entrevistas

Tabla 2.Entrevista 2. Nombre: Abgda. Claudia Silva Resumen de la entrevista:

Durante la entrevista con la abogada Claudia Silva, se discutió la creciente preocupación sobre la extorsión que utiliza imágenes generadas por IA. Silva expresó que las leyes en Ecuador, aunque abordan aspectos como el chantaje y la protección de la privacidad, no tratan específicamente los desafíos que presentan las imágenes digitales creadas artificialmente. Esta laguna legal limita la capacidad del sistema judicial para manejar estos casos de manera efectiva. Propuso que se consideren reformas legislativas para definir claramente estos nuevos tipos de delitos y enfatizó la importancia de educar y capacitar a los profesionales del derecho en temas de derecho digital. Silva subrayó que, además de actualizar las leyes, es crucial contar con una respuesta legal ágil y eficaz que pueda adaptarse rápidamente a los avances tecnológicos, protegiendo así de manera más efectiva a las personas afectadas.

Autor: Karla Pacheco

Tapia Fuente: Entrevistas

Tabla 3. Entrevista 3. Nombre: Ing. Carlos Ortiz

Resumen de la entrevista:

En la entrevista con el Ingeniero Carlos Ortiz, experto en IA, se exploró cómo las imágenes creadas con tecnologías avanzadas están complicando el panorama legal actual. Ortiz explicó que las redes generativas adversariales (GANs) pueden producir imágenes tan realistas que resulta difícil distinguirlas de las auténticas, lo que representa un desafío considerable cuando estas imágenes se utilizan para extorsionar a personas. Destacó que muchas leyes aún no están preparadas para lidiar con estas nuevas tecnologías y sugirió que es urgente actualizar las normativas para incluir regulaciones específicas sobre el uso y la creación de imágenes sintéticas. Además, mencionó la necesidad de desarrollar sistemas que puedan verificar la autenticidad de las imágenes y recomendó una colaboración más estrecha entre tecnólogos y legisladores para abordar estos problemas de manera efectiva.

Autor: Karla Pacheco Tapia

Fuente: Entrevistas

Tabla 4. Entrevista 4. Nombre: Xavier Villa

Resumen de la entrevista:

En la entrevista con Xavier Villa, experto en ciberseguridad con conocimientos en IA, se discutió cómo las imágenes generadas por IA están siendo utilizadas para extorsionar a personas y cómo esto desafía las leyes actuales. Villa explicó que el rápido avance de la tecnología ha superado la legislación vigente, dejando a las víctimas desprotegidas. Enfatizó que, para abordar este problema, es fundamental que las leyes se adapten al ritmo de la tecnología. Propuso que las normativas incluyan cláusulas específicas sobre el uso indebido de IA para crear imágenes comprometedoras y que se desarrollen métodos para identificar y rastrear estas imágenes falsas. Villa también resaltó la importancia de educar tanto a usuarios como a profesionales del derecho sobre las últimas amenazas en ciberseguridad para construir una respuesta más sólida ante estos delitos emergentes.

Autor: Karla Pacheco

Tapia Fuente: Entrevistas

Estas entrevistas reflejan la necesidad urgente de adaptar el marco legal y educativo a los rápidos avances tecnológicos, garantizando una protección efectiva contra los delitos cibernéticos emergentes.

4.1.1.1. Análisis de las entrevistas

Para analizar la información recopilada, se establecieron códigos o criterios de optimización alineados con los objetivos definidos, con el fin de identificar en cada respuesta de los entrevistados los datos relevantes que contribuyan a alcanzar dichos objetivos. A continuación, se presenta el análisis de los comentarios de las entrevistas, basándose en los códigos generados, los cuales fueron recurrentes y significativos entre los participantes, permitiendo avanzar en nuestra investigación.

Código: Experiencia y formación

legal Comentario de los entrevistados:

Los entrevistados coinciden en que la implementación de la inteligencia artificial (IA) en los procedimientos administrativos busca mejorar la eficiencia y eficacia, reduciendo la carga laboral, optimizando los tiempos de respuesta y garantizando la seguridad de la información generada por los sistemas. Se reconoce que la burocracia tradicional puede desmotivar a los ciudadanos debido a procesos complejos y lentos; por ello, la IA podría sustituir parcialmente la intervención humana mediante algoritmos, simplificando trámites y aumentando la confianza en la administración pública. Los participantes creen que la IA puede ofrecer respuestas rápidas y eficientes en comparación con los procesos burocráticos tradicionales, y consideran que su utilidad se limita a ciertos casos, como la gestión de expedientes y la catalogación de información, destacando su capacidad para recopilar, resumir y proporcionar acceso eficiente a grandes volúmenes de datos relevantes, como sentencias judiciales y casos previamente resueltos. En resumen, todos reconocen el potencial de la IA para optimizar los procedimientos administrativos y mejorar la experiencia ciudadana con la administración pública.

Código: Casos relacionados con inteligencia artificial

Comentario de los entrevistados:

Los participantes coinciden en la necesidad y el potencial de integrar la IA, destacando su capacidad para automatizar tareas repetitivas y mejorar la eficiencia en la administración pública. Se enfatiza su utilidad en la gestión de datos públicos y la formulación de políticas, así como en la optimización de la burocracia y el análisis de información legal. Se proyecta un futuro donde la IA brinde una ayuda significativa en la gestión de la información y en la toma de decisiones administrativas, especialmente con el desarrollo de sistemas de gobierno electrónico más avanzados. En este sentido, la gestión de expedientes y la catalogación de información emergen como áreas clave donde la IA puede facilitar un acceso más eficiente y completo a los datos almacenados por la administración. En resumen, los entrevistados ven la IA como una herramienta esencial para mejorar la calidad y agilidad de los procesos administrativos en diversas áreas de la gestión estatal.

Código: Legislación y jurisprudencia

relevante Comentario de los entrevistados:

Los participantes expresan la necesidad de establecer normativas claras que regulen el funcionamiento de los sistemas de IA en los procedimientos administrativos, alineándolos con la legislación vigente. Destacan la importancia de implementar medidas y controles para garantizar la calidad y veracidad de los datos utilizados en estos sistemas, así como la necesidad de un marco legal sólido que asegure su uso ético y responsable, protegiendo los derechos y la seguridad ciudadana. Se argumenta que el desarrollo de la IA debe ir acompañado de políticas que permitan su viabilidad y regulación, especialmente en el sector público, considerando la protección de datos personales y el enfoque en la mejora de los servicios públicos. Además, se subraya la importancia de establecer límites de responsabilidad y competencia para la IA en la administración pública, así como la objetividad y revisión rigurosa de la información utilizada en la toma de decisiones. En resumen, los entrevistados abogan por normativas que aseguren un uso ético, efectivo y responsable de la IA en los procedimientos administrativos, considerando aspectos legales, de protección de datos y de mejora de los servicios públicos.

Código: Elementos clave en juicios

Comentario de los entrevistados:

En las reflexiones de los participantes se destaca la preocupación por la desnaturalización en el uso de la IA en los procedimientos administrativos, particularmente en la vulnerabilidad de datos privados y la posibilidad de extrapolación hacia otros intereses. Se subraya la importancia de proteger la privacidad y evitar la creación de perfiles que puedan sesgar el funcionamiento de la IA. Se resalta la necesidad de regular la tecnología para garantizar su uso justo y equitativo, evitando la perpetuación de sesgos y discriminaciones. Asimismo, se reconoce el potencial de la IA como herramienta, pero se advierte sobre la importancia de no convertirla en un fin en sí misma, sino en un medio para servir a la comunidad y efectivizar los derechos fundamentales de las personas. En resumen, se aboga por un enfoque ético, responsable y regulado en el empleo de la IA en la administración pública.

Código: Responsabilidad legal

Comentario de los entrevistados:

Los participantes resaltan la importancia de garantizar la calidad, eficiencia y eficacia en la administración pública, así como el desafío ético de utilizar la IA como una herramienta complementaria al raciocinio humano. Se destacan beneficios como la disminución de la carga laboral, la optimización de los tiempos de respuesta y la mejora en la seguridad y respaldo de la información. Se enfatiza la necesidad de que la IA sea una herramienta que complemente y no reemplace el análisis humano, además de la importancia de mantener la calidad y precisión en las respuestas generadas. La implementación exitosa de la IA requerirá un enfoque estratégico, cambios culturales y políticas sólidas. En resumen, se reconoce el potencial de la IA para mejorar la eficiencia y efectividad de los procedimientos administrativos, pero se subraya la importancia de mantener la calidad, la transparencia y el respeto por los principios de buena gobernanza en la administración pública.

Código: Desafíos técnicos y métodos de autenticación

Comentario de los entrevistados:

Los participantes en Ecuador muestran una variedad de perspectivas sobre la implementación de la IA en la administración pública. Se reconoce que la IA puede mejorar la eficiencia y la transparencia de los procedimientos administrativos al estandarizar procesos repetitivos, pero se subraya la necesidad de recursos y un marco legal sólido para garantizar su uso ético y responsable. Aunque algunos creen que la implementación de la IA es factible y podría generar beneficios significativos, otros advierten sobre desafíos culturales y resistencia al cambio tecnológico. Sin embargo, se reconoce el potencial de la IA para recopilar y resumir grandes cantidades de información, facilitar el acceso a datos relevantes y mejorar la toma de decisiones administrativas a largo plazo, a pesar de los obstáculos inmediatos. En general, se considera que la IA puede ser una herramienta valiosa para mejorar la administración

4.2. Interpretación de los resultados

La Figura 2 presenta una red semántica que ilustra la responsabilidad legal en casos de extorsión mediante imágenes generadas por inteligencia artificial (IA). Este

gráfico destaca dos categorías principales: los actores involucrados y los factores determinantes que influyen en la atribución de responsabilidad.

Actores Involucrados:

Perpetrador: Individuo que utiliza imágenes generadas por IA con fines de extorsión. Su intención y conocimiento sobre el uso indebido de la tecnología son fundamentales para determinar su responsabilidad legal.

Desarrolladores de IA: Profesionales que crean herramientas de generación de imágenes. Aunque no participan directamente en el acto delictivo, su responsabilidad radica en implementar medidas preventivas y salvaguardas para evitar el uso malintencionado de sus tecnologías.

Factores Determinantes:

Intención del Perpetrador: Comprender la motivación detrás del uso de imágenes generadas por IA es esencial para evaluar la gravedad del acto y la responsabilidad asociada.

Conocimiento del Usuario: La conciencia y comprensión del usuario sobre los riesgos y las implicaciones legales del uso de IA son cruciales. La falta de conocimiento puede influir en la evaluación de la responsabilidad.

Salvaguardias Implementadas: Las medidas de seguridad y protocolos establecidos por los desarrolladores de IA para prevenir usos indebidos son determinantes. La ausencia o insuficiencia de estas medidas puede aumentar la responsabilidad de los creadores de la tecnología.

Este análisis sugiere que la responsabilidad en casos de extorsión con IA es compartida. Los perpetradores son responsables por sus acciones directas, mientras que los desarrolladores de IA tienen la obligación de diseñar sistemas seguros que minimicen el riesgo de uso malintencionado. La educación y concienciación de los usuarios sobre los riesgos asociados con la IA también juegan un papel vital en la prevención de estos delitos.

La colaboración entre tecnólogos, legisladores y profesionales legales es esencial para abordar los desafíos que presenta la IA en el ámbito legal. Establecer un marco legal sólido y actualizado es crucial para proteger a las víctimas y promover el uso ético de la inteligencia artificial.

En Ecuador, el Código Orgánico Integral Penal (COIP) aborda la extorsión en su artículo 185, estableciendo sanciones para quienes, con violencia o intimidación, obliguen a otro a realizar u omitir un acto en perjuicio de su patrimonio o el de un tercero. La adaptación de estas normativas a los desafíos que presenta la IA es un paso necesario para garantizar una respuesta legal efectiva ante estos delitos emergentes.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Analizar a fondo las ideas teóricas y las leyes que tienen que ver con la extorsión y el uso de imágenes hechas con inteligencia artificial nos ha dado una buena base para entender cómo la ley ecuatoriana trata este tema. Si bien lo que ya se sabe y las decisiones de los jueces nos ayudan a entender los puntos clave del delito de extorsión, la tecnología avanza muy rápido, y usar la inteligencia artificial para crear imágenes plantea nuevos problemas legales que las leyes de Ecuador todavía no cubren bien. Por eso, es importante actualizar las leyes para que hablen directamente sobre cómo se usa la inteligencia artificial para crear y compartir imágenes falsas con el fin de extorsionar.

El impacto de usar imágenes creadas por inteligencia artificial en los casos de extorsión en Ecuador es cada vez mayor. Aunque las leyes actuales mencionan cosas relacionadas con la extorsión y los delitos informáticos, hemos encontrado que faltan partes importantes en las leyes sobre el uso de imágenes hechas por IA. Estas faltas hacen que sea difícil responder bien a estos nuevos tipos de delitos. Por lo tanto, es urgente revisar y cambiar las leyes ecuatorianas para enfrentar estos problemas de una manera más precisa, para proteger mejor a las personas afectadas y hacer más fuertes los castigos para los culpables.

Al mirar cómo otros países han hecho sus leyes sobre delitos en internet y protección de datos, hemos encontrado ideas y leyes que se podrían usar en Ecuador para tratar los delitos de extorsión que involucran compartir imágenes creadas por inteligencia artificial. Lo que han hecho otros países, que ya tienen leyes específicas para regular el uso de la inteligencia artificial y proteger la información personal, nos enseña cosas importantes para fortalecer las leyes ecuatorianas. Esta forma de comparar nos dice que necesitamos tener un conjunto de leyes completo que incluya formas de prevenir estos delitos, castigos claros para quienes los cometen y un buen sistema para proteger a las víctimas, para que la ley pueda responder mejor a estos delitos.

Finalmente, este trabajo subraya que solo trabajando juntos y entre varios sectores se puede enfrentar de verdad el difícil problema de la extorsión con imágenes creadas por IA. La ayuda mutua entre diferentes partes de la sociedad es clave para una respuesta que funcione.

5.2 Recomendaciones

Crear leyes específicas para enfrentar los problemas únicos que trae la extorsión con imágenes hechas por inteligencia artificial (IA). Estas leyes deberían decir claramente quién es responsable, tanto los que cometen el delito como los que crean la IA, y asegurar que haya castigos claros y que realmente sirvan. Para que la IA se use bien y de forma ética en el gobierno y en las oficinas, se sugiere crear un plan nacional de inteligencia artificial. Este plan debería tener instrucciones detalladas para que el gobierno funcione mejor y sea más transparente, protegiendo los derechos de las personas y apoyando la investigación y creación de tecnologías de IA que se ajusten a lo que necesitamos.

Es muy importante que las personas que trabajan en el gobierno y la policía aprendan continuamente sobre cómo se usa y se regula la IA. Además, se recomienda hacer campañas para que la gente sepa los peligros y las consecuencias legales de usar mal la IA, promoviendo un uso seguro y ético. Se debería invertir en mejorar las formas de rastrear y perseguir digitalmente a quienes extorsionan con imágenes creadas por IA para poder encontrarlos y llevarlos ante la justicia. Esto significa capacitar en técnicas para encontrar pruebas digitales y mejorar la tecnología que se necesita para esto.

Se recomienda poner reglas que obliguen a las empresas de tecnología y a quienes crean la IA a tener medidas de seguridad para evitar que las imágenes generadas por IA se usen mal. Es muy importante que estas empresas trabajen junto con las autoridades para poder responder bien a estos delitos. Es vital tener normas de seguridad estrictas para cómo se crea y se usa la IA, incluyendo protecciones desde el principio. Estas normas deberían ser obligatorias para quienes desarrollan y ofrecen plataformas de IA, asegurando que la tecnología se use de manera segura y responsable.

BIBLIOGRAFÍA

Asamblea Nacional. (2014). Código Orgánico Integral Penal. Registro Oficial.

Asamblea Nacional. (2021). Ley de Protección de Datos Personales. Registro Oficial.

Bartneck, C., & Suzuki, T. (2020). Defining synthetic media. Journal of Visual Languages & Computing, 61, 100503.

Brown, A. (2021). Global perspectives on AI-generated image extortion: Legal challenges and responses. Journal of Technology Law, 15(2), 195-210. Brown, A., Johnson, C., & Smith, D. (2024). Digital forensics in the age of AI: Challenges and opportunities. Journal of Cybercrime Law, 15(2), 68-85.

California Courts. (2014). People v. Bollaert. Superior Court of California.

Cámara Nacional en lo Criminal y Correccional. (2016). Caso Aciar. Buenos Aires, Argentina.

Congresso Nacional. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União.

Chen, L. (2024). Public understanding of AI: A key factor in preventing misuse. Tech Ethics Review, 7(3), 87-102.

Consejo de Europa. (2001). Convenio de Budapest sobre Cibercriminalidad. Estrasburgo.

Cortes Generales. (2018). Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales. Madrid.

Davis, C. (2020). Platform responsibilities in combating AI-generated image extortion. Technology Ethics Quarterly, 8(4), 225-240.

García, M. (2023). Transnational cybercrime and AI: A legal perspective. International Journal of Technology Law, 11(4), 195-210.

Gómez, J. (2022). La actualización legislativa en el contexto de la tecnología y la IA. Revista de Derecho Penal y Criminología, 8(3), 45-62.

Gómez, R. (2022). La Adaptación de las Leyes de Extorsión en la Era Digital. Revista de Derecho Penal.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... Bengio, Y. (2014). Generative adversarial nets. In Advances in Neural Information Processing Systems (pp. 2672-2680).

Greenberg, L. (2021). Legal complexities in cases of AI-generated image extortion. In K. White (Ed.), Ethics and Artificial Intelligence (pp. 40-58). New York: Academic Press.

Jones, R. (2023). Legislative approaches to addressing AI-generated image extortion: A comparative analysis. Journal of Legal Technology, 27(1), 70-85.

Johnson, R., & Lee, S. (2022). Developer responsibility in AI-enabled crimes. AI and Society, 37(2), 120-135.

Karnatak High Court. (2019). X vs. State of Karnataka. Bengaluru, India.

Li, Y., Chang, M.-C., Lyu, S., & Fu, K. (2018). In the wild: Deep learning-based fake news detection on social media. IEEE Intelligent Systems, 33(5), 76-81.

Liu, Y., & Deng, Z. (2020). A survey of deepfake detection techniques. Journal of Multimedia Tools and Applications, 79(9-10), 111-132.

Organización de los Estados Americanos. (1969). Convención Americana sobre Derechos Humanos. San José, Costa Rica.

Roberts, E. (2023). Emerging jurisprudence in AI-related extortion cases. Law and Technology Review, 9(3), 140-158.

Smith, P. (2022). Challenges in applying defamation and privacy laws to AI-generated image extortion cases. International Journal of Law and Technology, 12(3), 110-125.

Smith, J. (2023). The legal landscape of AI-generated imagery. Cyber Law Journal, 28(1), 40-55.

Tan, Z., Liu, D., Luan, B., & Zhu, X. (2021). Deep learning and its applications in biometrics. IEEE Transactions on Emerging Topics in Computational Intelligence, 5(5), 761-773.

Tribunal Penal de Pichincha. (2021). Caso de Extorsión Cibernética. Quito, Ecuador.

Tribunal de Justicia de la Unión Europea. (2014). Google Spain SL v. Agencia Española de Protección de Datos. Luxemburgo.

Tribunal Supremo de España. (2021). [Caso Anónimo].
Código Orgánico Integral Penal de Argentina. (2020). [Caso Anónimo].

Tribunal Superior de Justicia de Brasil. (2021). [Caso Anónimo].

UK Courts. (2000). R v. Bowden. London, UK.

UK Court of Appeal. (2019). Interpretación de la Ley de Justicia Criminal y Tribunales de 2015. Londres, Reino Unido.

US Court of Appeals. (2014). United States v. Osinger. Washington, D.C.

US Congress. (1986). Computer Fraud and Abuse Act. Washington, D.C.

Williams, K., & Thompson, P. (2022). Balancing innovation and regulation in AI development. Tech Policy Quarterly, 18(2), 50-65.