

**UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS  
SOCIALES Y POLÍTICAS**

**CARRERA DE DERECHO**

**TEMA:**

**“Delito de Estafa mediante el uso tecnológico del Deepfake”**

**AUTORA:**

**Cabrera Loor, Ana Cristina**

**Trabajo de Titulación previo a la obtención del grado  
de ABOGADA**

**TUTOR:**

**Ab. Carrión Carrión, Pablo Javier, Mgs.**

**Guayaquil, Ecuador**

**20 de febrero de 2025**



**UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL**

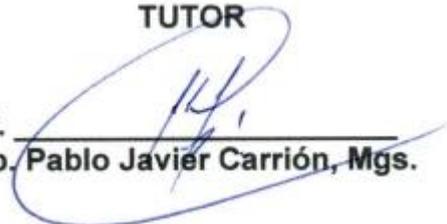
**FACULTAD DE JURISPRUDENCIA Y CIENCIAS  
SOCIALES Y POLÍTICAS**

**CARRERA DE DERECHO**

**CERTIFICACIÓN**

Certificamos que el presente trabajo titulación, fue realizado en su totalidad por **Cabrera Loor, Ana Cristina**, como requerimiento para la obtención del Título de Abogada.

**TUTOR**

f.   
Ab. Pablo Javier Carrión, Mgs.

**DIRECTORA DE LA CARRERA**

f. \_\_\_\_\_  
**Dra. Nuria Pérez Puig-Mir, Mgs**

**Guayaquil, a los 20 días del mes de febrero del año 2025**



**UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS  
SOCIALES Y POLÍTICAS**

**CARRERA DE DERECHO**

**DECLARACIÓN DE RESPONSABILIDAD**

**Yo, Cabrera Loor, Ana Cristina**

**DECLARO QUE:**

El Trabajo de Titulación, **Delito de Estafa mediante el uso tecnológico del Deepfake**, previo a la obtención del Título de **Abogada**, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

**Guayaquil, a los 20 días del mes de febrero del año 2025**

**AUTORA**

f. \_\_\_\_\_

**Cabrera Loor, Ana Cristina**



**UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS  
SOCIALES Y POLÍTICAS**

**CARRERA DE DERECHO**

**AUTORIZACIÓN**

**Yo, Cabrera Loor, Ana Cristina**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación: **Delito de Estafa mediante el uso tecnológico del Deepfake**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

**Guayaquil, a los 20 días del mes de febrero del año 2025**

**AUTORA**

f. \_\_\_\_\_  
**Cabrera Loor, Ana Cristina**



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS  
SOCIALES Y POLÍTICAS

URKUND

**CERTIFICADO DE ANÁLISIS**  
magister

**ANA CRISTINA CABRERA  
COMPILATIO 2 (1)**

**5%**  
Textos sospechosos

- 4: Similitudes  
0: similitudes entre comillas (ignorado)  
0: entre las fuentes mencionadas (ignorado)
- 2: Idiomas no reconocidos (ignorado)
- 2: Textos potencialmente generados por la IA (ignorado)

Nombre del documento: ANA CRISTINA CABRERA COMPILATIO 2 (1).docx	Depositante: Paola María Toscanini Sequeira Fecha de depósito: 14/2/2025 Tipo de carga: interface fecha de fin de análisis: 14/2/2025	Número de palabras: 4052 Número de caracteres: 26.290
ID del documento: 69f9a671e4ee5b72b5c537e1f988c6af66f		
Tamaño del documento original: 256,17 KB		
Autores: []		

Ubicación de las similitudes en el documento:

TUTOR

f.   
Ab. Pablo Javier Carrión, Mgs.

AUTORA

f.   
Cabrera Loo, Ana Cristina

## **AGRADECIMIENTO**

Agradezco a Dios quien me ha guiado en cada paso que he dado para llegar hasta aquí. A mi familia y amigos y todos quienes de una u otra manera contribuyeron en todo mi trayecto académico, el cual ahora es un logro profesional y personal

Con gratitud,

Cabrera Loor, Ana Cristina

## **DEDICATORIA**

A mis padres quienes me han formado con valores, quienes me ha apoyado con su amor incondicional y a quien debo mi desarrollo académico.

A mis hijas por la motivación para nunca rendirme y seguir adelante en cada uno de mis proyectos

Los amo,

Cabrera Loor, Ana Cristina



**UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS  
SOCIALES Y POLÍTICAS**

**TRIBUNAL DE SUSTENTACIÓN**

f. \_\_\_\_\_

**DR. LEOPOLDO XAVIER ZAVALA EGAS, MGS.**

DECANO

f. \_\_\_\_\_

**DRA. ANGELA MARIA PAREDES CAVERO.**

COORDINADOR DEL AREA

f. \_\_\_\_\_

**AB. EDUARDO MONAR, MGS.**

OPONENTE



**UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS  
SOCIALES Y POLÍTICAS**

**Facultad: Jurisprudencia**

**Carrera: Derecho**

**Periodo: UTE B 2024**

**Fecha: 07 de febrero del 2025**

**ACTA DE INFORME FINAL**

El abajo firmante, docente tutor del Trabajo de Titulación denominado “Delito de Estafa mediante el uso tecnológico del Deepfake” elaborado por la estudiante **ANA CRISTINA CABRERA LOOR**, certifica que durante el proceso de acompañamiento dicha estudiante ha obtenido la calificación de 10 (DIEZ), lo cual la califica como **APTA PARA LA SUSTENTACIÓN**.

**TUTOR**

f.   
Ab. Pablo Javier Carrión, Mgs.

# ÍNDICE GENERAL

AGRADECIMIENTO .....	VI
DEDICATORIA .....	VII
ÍNDICE GENERAL.....	X
RESUMEN.....	XI
ABSTRACT.....	XII
Introducción .....	2
DESARROLLO .....	3
CAPITULO I: Elementos Conceptuales .....	3
CAPÍTULO II: Resoluciones sobre Casos del Deepfake en Ecuador .....	10
Exposición del Problema Jurídico .....	14
PROPUESTA DE REFORMA AL COIP.....	16
CONCLUSIONES Y RECOMENDACIONES.....	19
BIBLIOGRAFÍA.....	20

## RESUMEN

Se ha llevado a cabo la elaboración del presente documento académico sobre “Delito de Estafa mediante el uso tecnológico del Deepfake”, debido al alto número de estafas transcurridas en el año 2024, utilizando el método Deepfake en plataformas digitales; ya que el problema es que en estos casos el sistema de justicia ecuatoriana lo sanciona solo como una aproximación concurrente de suplantación de identidad.

Se destaca la importancia del transformar el cuerpo legal desarrollando un marco jurídico robusto dentro del Código Orgánico Integral Penal, en el cual se introduzca o tipifique un artículo de las particularidades que se dan mediante Deepfake como un delito autónomo en el COIP y así se pueda sancionar y prevenir el uso indebido de este método mediante un procedimiento eficaz del sistema de justicia.

**Palabras Claves:** Estafa, Deepfake, plataformas digitales, procedimiento eficaz.

## ABSTRACT

The present academic document on “Crime of Fraud through the technological use of Deepfake” has been prepared due to the high number of scams that occurred in 2024, using the Deepfake method on digital platforms; since the problem is that in these cases the Ecuadorian justice system sanctions it only as a concurrent approximation of identity theft.

The importance of transforming the legal body by developing a robust legal framework within the Comprehensive Organic Criminal Code is highlighted, in which an article of the particularities that occur through Deepfake is introduced or classified as an autonomous crime in the COIP and thus the misuse of this method can be sanctioned and prevented through an effective procedure of the justice system.

**Keywords:** Fraud, Deepfake, digital platforms, effective procedure.

## Introducción

La presente investigación analiza el delito de estafa mediante el uso tecnológico del Deepfake, llevado a cabo por la situación actual que enfrenta Ecuador, donde la tecnología se convierte en herramienta también de los delincuentes que aplican la modalidad de ultra falsificación y deepfake, utilizando contenido de video, audio o imagen en que aparecen personas que pueden ser reales o ficticias, manipulando voces, para obtener beneficios de diferentes indoles que involucran delitos penales como el de estafa.

La situación anteriormente descrita causa un impacto negativo, considerando que ha abierto las puertas hacia este nuevo tipo de delito, causando afectación directa a personas quienes por ejemplo realizan compras en plataformas digitales, las mismas que inclusive utilizan audios para asegurarse de dicha compra; pero, sin embargo, igualmente son estafados, tema que afecta el patrimonio económico y uso de datos personales.

Consecuentemente, el problema es que en Ecuador este hecho delictivo se reprime penalmente bajo la figura de suplantación de identidad establecida en el artículo 212 del Código Orgánico Integral Penal (COIP); es decir en estos casos el sistema de justicia del país lo hace solo haciendo una aproximación, evidenciándose un vacío normativo.

De lo dado a conocer, genera la necesidad del análisis a doctrinas y normativas penales de esta modalidad de estafa, reflejado en el capítulo I y II con la finalidad de evidenciar que en el marco ecuatoriano no existe la tipificación del delito del Deepfake, por lo cual, es necesaria su incorporación en el marco jurídico siendo este el problema jurídico, al no existir en el país una actuación efectiva de las entidades de prevención y sanción del delito bajo la modalidad de ultra falsificación y deepfake.

## DESARROLLO

### CAPITULO I: Elementos Conceptuales

#### 1.1. *Estafa*

La doctrina, se refiere al delito de estafa, como la apropiación de bienes por medios fraudulentos que infundan esperanza o temor y al referirse a la estafa, el Dr. Efraín Torres, en su obra breves comentarios al COIP del Ecuador.

*Estafar es, pedir o sacar dinero en modalidades nuevas, masificación del internet, debido a que redes sociales han potenciado esta capacidad de la captación de un gran número de víctimas, ya que basta con poseer una cuenta dentro de una plataforma digital X para que distintos estafadores lleguen inmediatamente a miles y miles de personas a cuestión de segundo u horas, estos delincuentes evaden controles de prevención los cuales en la antigüedad eran más difíciles. (Torres, 2020, pág. 108)*

Mientras que para el doctrinario James Reátegui la estafa penal se trata de la necesidad de una justicia penal que sea ágil en la nueva era digital; debido a que basta con una cuenta dentro de una plataforma digital en que los estafadores mediante online llegan a miles de personas inmediatamente en cuestión de horas, minutos e inclusive segundos, por lo que se debe contemplar esta nueva modalidad delictiva de estafa, reconociendo actualización del marco penal; y, últimamente, es común observarse mediante redes sociales a la proliferación de los ofrecimientos mágicos de ofertas, para volverse estos estafadores millonario en un abrir y cerrar de ojos, invitando a participar a sus víctimas de supuestos negocios de inversión exclusiva para lograr aquellos ingresos extraordinarios, encubriendo, inclusive maniobras defraudatorias llamado Ponzi. (Reátegui, 2016)

El delito de estafa es uno de los delitos contra la propiedad; y, esencialmente, consiste en el ardid o engaño utilizando contenido de video, audio o imagen el agente activo, para provocar el error en la víctima, el estafador cree una persona falsa para formar una relación de negocios con un objetivo, y finalmente le convence que realice y envíe el dinero a una determinada cuenta bancaria; únicamente esta armado mediante inteligencia artificial aprovechándose de la confianza. (Zavala, 1988)

## **1.2. Ultra falsificación y Deepfake**

La definición de "deepfake y ultrafalsificación" inicia a mediados del año 2017 derivado de "Deep" cuyo significado es (profundo) y "fake" que significa (falso). El primero se enmarca en "deeplearning" conocido como aprendizaje profundo de la de inteligencia artificial, con técnica avanzada de algoritmos complejos, para crear ya sean videos o audios engañosos que parecen reales, por lo cual existen personas capaces del efectuar el engaño fácilmente con el objetivo de obtener un beneficio económico para sí mismo. (Oliva, 2022)

En la sociedad actual hay cibercriminales que usan la tecnología de ultrafalsificación y deepfake, como plataforma digital en donde vulneran cuentas de redes sociales para efectuar estafas de criptomonedas o beneficiarse económicamente por engañosas ventas online, es decir haciendo uso de ultrafalsificaciones o deepfakes, que son esos vídeos o audios en los que alguien se hace pasar por otra persona, aparentando que esta dice o hace unas cosas que, por razones obvias, ni ha dicho ni ha hecho. (Iglesias, 2024)

El uso indebido de los deepfakes y ultrafalsificaciones debido a que pueden replicar mediante el uso de plataformas digitales con precisión una apariencia y voz de la víctima, generando serias preocupaciones en el ámbito penal de cada país; que si bien es cierto que actualmente esta tecnología posee un gran potencial en aplicaciones innovadoras y creativas, que consecuentemente existirán riesgos legales, los cuales deben ser considerados dentro de los cuerpos penales. (Hao, 2020)

### **1.3. Clases de Deepfake**

Aunque el Deepfake son cada vez más sofisticados y son capaces de generar vídeos en los que se combina el audio y la imagen, aún podemos hablar de dos clases de Deepfake que son las siguientes:

#### **1.3.1. Deepface**

Consiste el DeepFace en una biblioteca Python de reconocimiento facial, análisis de aquellos atributos faciales, incluyendo por edad, el género, emociones en general y etnia; entre varios modelos del reconocimiento facial esta DeepFace, ArcFace, Dlib, y GhostFaceNet. Al permitir un exacto reconocimiento facial de alta precisión, detallando sus atributos, es que un grupo delictivo realiza estafas al aporvecharse de este nuevo sistema. (Oliva, 2022)

Esta tecnología puede ejecutar DeepFace para llevar a cabo estafas económicas y con solo unas pocas líneas de código, y simplemente importa la biblioteca y pasa la ruta de imagen exacta como entrada; obtiene acceso a un conjunto de funciones: Verificación facial, Reconocimiento facial, Análisis de atributos faciales y Análisis de rostros en tiempo real con transmisión de video. (Hao, 2020)

#### **1.3.2. Deepvoice**

Transformar texto en voces profundas realistas para realizar estafas se ha vuelto más fácil con los generadores de voz profunda de IA realistas. La voz profunda de IA está transformando la creación de contenido, ofreciendo voces realistas para videos, podcasts y mucho más. (Iglesias, 2024)

La creatividad actual impulsada por IA de generadores de voz profunda de IA para ayudarlo a crear voces increíbles, tal como CapCut, Resemble AI, Natural Reader, Play HT. Herramienta que también es utilizada por delincuentes que estafan económicamente a sus víctimas al utilizar el Deepvoica para generar voces profundas de IA, debido a que admite más de trescientos cincuenta voces diferentes y tiene potentes funciones de edición. (Torres, 2020, pág. 108)

#### **1.4. Plataformas digitales**

Las plataformas digitales son utilizadas por persona jurídica o natural quienes ofertan bienes o servicios mediante plataformas digitales; sin someterse a las autoridades de los organismos de control del país; por lo tanto, en caso de producirse un conflicto sobre la entrega o no de un determinado bien o servicio, estas personas perjudicadas no pueden acceder a vías jurídicas de protección por parte del sistema judicial, debido a que existen casos, donde ni siquiera la víctima llega a conocer a la persona quien le vende y está del otro lado de la pantalla. (Creismer, 2019)

El uso generalizado a través de plataformas digitales en Ecuador, tales como Mercado Libre y OLX, donde realizan transacciones de tipo comercial, y que en va en aumento, proporcionándole a las personas su conveniencia del adquirir un bien o servicio para comprar o vender online; consecuentemente debido al acceso libre y abierto de estas plataformas digitales, es que hay riesgos de defraudación mediante engaño. (Gómez, 2022)

La finalidad de las plataformas digitales es proteger a víctimas de daños graves, cuando personas hacen el mal uso de esta tecnología a través del método del Deepfake, por lo cual cada país debe contar con una legislación sólida, como forma de evitar esta clase de engaño, ya que muchas veces llegan a ser utilizadas por los ciberdelincuentes quienes usan Deepfake para llegar a engañar a las posibles víctimas, que a la vez se benefician económicamente y roban sus datos personales. (Acosta, 2024)

### **1.5. Bien jurídico protegido**

El bien jurídico protegido es la situación de dominio que tienen las personas sobre su patrimonio, el cual, puede ser objeto de un perjuicio producto de una situación delictiva, en virtud de que este ilícito se perfecciona al momento en que el agente obtiene un provecho económico indebido, esto es cuando dispone del patrimonio de su víctima, con la intención de incrementar el suyo a costa de un perjuicio ajeno. (Cornejo, 2023)

Respecto al hecho punible relacionado con la estafa se establece como bien jurídico protegido, el patrimonio individual, el cual Bustamante (1979) define, como la universalidad jurídica que engloba bienes, derechos y obligaciones del cual es titular un individuo y por ende que puede disponer de él voluntariamente. Asimismo, resalta que el patrimonio no solo engloba dinero sino también cosas, créditos, derechos reales, personales e intelectuales y, todo aquello que es susceptible de ser valorado económicamente. (Pons, 2019)

En el delito de estafa el bien jurídico protegido es el patrimonio constituido por el conjunto de bienes o valores que son cuantificables económicamente. Peña (2010), citado por Reátegui (2015); indica que en la doctrina especializada se sostiene que el bien jurídico protegido en el delito de estafa es el patrimonio de una persona, que se ve afectado por la conducta engañosa del victimario, Asimismo, Buompadre (2012); indica que la doctrina mayoritaria ha establecido que el bien jurídico afectado por este ilícito son los elementos integrantes del patrimonio.

### **1.6. Anonimato del sujeto activo en delito de estafa a través del método Deepfake.**

Para Villazón (2021), "El anonimato es aquella condición que posee una persona para poder esconder su identidad" (p.87). Esta definición refiere a la situación que se genera producto del ocultamiento de características que permitan la identificación de la persona que realiza una determinada acción.

En el caso materia de investigación se tiene al anonimato como una ventaja propia de la privacidad que ofrece el internet la cual provee a los ciberdelincuentes de circunstancias de clandestinidad que les permite realizar sus hechos ilícitos sin dejar rastro alguno. Sin embargo, se afirma que el anonimato en esta era tecnológica representa un derecho digital que se desprenden de los derechos fundamentales clásicos como; la privacidad, la intimidad y la libre expresión, los cuales representan características que poseen los usuarios del Internet para que su identidad permanece oculta o reservada ante otros individuos que utilizan la red.

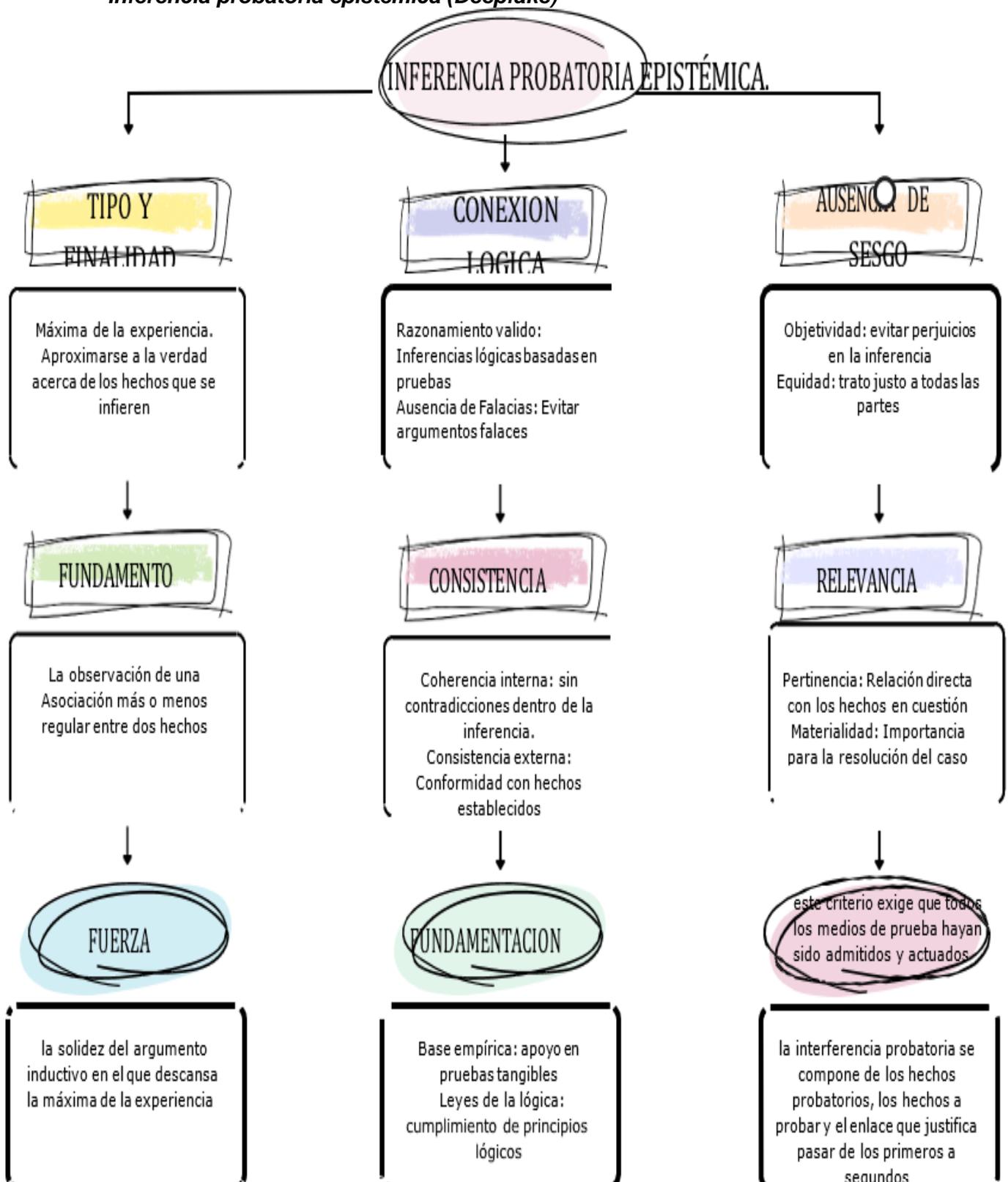
Lo que resulta preocupante en torno al derecho al anonimato es la ausencia de reglas, pues, lo que busca el internet es dar esa libertad que en la realidad física no se posee, ya que, en el mundo real parte de nuestra identidad queda revelada independientemente de nuestra voluntad en cambio en el ciberespacio, la situación es totalmente diferente, puesto que, no existe obligación de mostrar una identidad, ya que, lo único que nos distingue es un COIP siendo, un elemento esencial para mantener el anonimato en la Red. (Agustinoy, 2016)

### **1.7. Inferencia Probatoria Epistémica**

En el complejo entramado del COIP, la inferencia probatoria epistémica emerge como un componente esencial para establecer conexiones sólidas entre el delito imputado y el individuo; por lo que es el valorar la prueba que consiste en un razonamiento según el cual se evalúan en qué medida los elementos de juicio, de los hechos probatorios avalan la hipótesis de los elementos de convicción del delito de Deepfake que se quiere probar. (Pons, 2019)

La función de la deliberación y relevancia de la inferencia probatoria epistémica para la calidad del razonamiento probatorio en delito de Deepfake, al menos en Ecuador, no ha sido del todo destacada frente a la atención de denuncias de víctimas de estafa bajo esta modalidad en fiscalía; y, para mejor comprensión se muestra la siguiente gráfica:

**Grafica No. 1:**  
**Inferencia probatoria epistémica (Deepfake)**



**Fuente:** Twomey J, Ching D, Aylett MP, Quayle M, Linehan C. Deepfake videos undermine our epistemic. Obtenido de (Twomey J. Inferencia probatoria epistémica. <https://doi.org/10.1371/journal.pone.0291668>, 2023).

## **CAPÍTULO II: Resoluciones sobre Casos del Deepfake en Ecuador**

### **2.1. Análisis Jurídico de Casos reflejados en Corte Nacional de Justicia**

Para llevar a cabo este estudio, se llevó a cabo la revisión de la Resolución No. 342-2017 del delito de estafa reflejado dentro del buscador de Jurisprudencia de Corte Nacional de Justicia del Ecuador (SIPJUR), y Tribunal de Garantías Penales, cuyos casos del delito de estafa utilizaron ultra falsificación y Deepfake engañando a sus víctimas para llevar a cabo dicha estafa, análisis jurídico imprescindible para conocer la manera de aplicación de la legislación vigente en Ecuador por autoridades del sistema de administración de justicia en estos casos.

#### **2.1.1. Resolución No. 342-2017 dictada por la Corte Nacional de Justicia**

La Sala de lo Penal Militar, Policial y Tránsito de Corte Nacional de Justicia con relación al Juicio No 0305-2016 dicto resolución No 342-2017 de fecha 16 de marzo del 2017, donde su importancia radica en que para este caso la Corte señala que se ha desvanecido el cargo casacional relativo a que el recurrente no adecuó su conducta al delito de estafa, sino al de abuso de confianza, pues el examen de la sentencia impugnada, arroja que los juzgadores de apelación, han establecido con precisión todos los elementos constitutivos del tipo penal de estafa, incluido el elemento subjetivo del dolo, entendido como el conocimiento y la voluntad de realizar el tipo objetivo del delito, con el que ha actuado el recurrente, sobre todo, porque este ha obtenido un beneficio patrimonial para sí mismo, mediante la simulación de hechos falsos utilizando contenido de video, audio o imagen; dada por plataforma digitales en que utiliza alta tecnología para suplantar el rostro y voz en el remate de un bien inmueble, producto de un juicio ejecutivo; y de esta forma ha inducido a error a la víctima, quien ha realizado un acto que ha perjudicado su patrimonio; por tanto, resulta inobjetable que el recurrente ha adecuado su conducta al ilícito de estafa tipificado y sancionado en el artículo 186 del Código Orgánico Integral Penal.

Uno de los actos ilícitos que configuran una estafa, consiste en hacerse entregar fondos con el propósito de apropiarse de los mismos, valiéndose de engaños e infundiendo falsas esperanzas sobre un acontecimiento quimérico.

Se evidencia un punto de inflexión del Deepfake en el Proceso No. 09908-2024-01981, de estafa mediante plataformas digitales por Ingrid Adriana S. N. donde la Fiscalía demostró que la procesada habría utilizado la red social Facebook utilizando contenido de video, audio o imagen, para hacerse pasar por un familiar de la víctima, beneficiándose económicamente la ahora sentenciada a 5 años, por el delito de estafa tipificado en el artículo 186 del COIP; más sin embargo los jueces competentes determinan únicamente una primera aproximación al concepto de la estafa, la cual consistió en el engaño a través del DeepfaKe.

Otro proceso en que también se evidencia es del No. 06101-2024-03013, de estafa ocurrida en Riobamba provincia de Chimborazo, donde Tribunal de Garantías Penales de Chimborazo sentenció a tres años y cuatro meses de privación de libertad al ciudadano José M., como autor directo del delito de estafa en que utilizo contenido de video, audio o imagen, para hacerse pasar por otro; y, efectivamente los jueces solo hacen una aproximación.

En el mismo sentido tenemos como el Proceso No. 17391-2024-0084275 en Quito provincia de Pichincha, el Tribunal de Garantías Penales de Pichincha que conoció el caso en que sentenció a Isabel P. a diez años de prisión por el delito de estafa masiva a más de 300 víctimas; es decir sentenciada por el delito de estafa tipificado en los incisos 1 y 3 del artículo 186 del COIP. En este caso, la conducta de la acusada que es sentenciada solo hace una aproximación los jueces competentes.

Concluyendo, de la revisión de casos por el delito de estafa de Corte Nacional de Justicia; y Tribunal de Garantías Penales; se permitió identificar el encuadre jurídico llevado a cabo por los administradores de justicia sobre los hechos del delito, elementos configuradores en dicha acción, determinando únicamente una aproximación cuando dictan sentencia a las personas imputadas dentro de cada caso de estudio.

Es preciso mencionar que la Constitución de la República del Ecuador, en los numerales 7 y 19 del artículo 66 reconocen el derecho de toda persona agraviada por informaciones, difamaciones sin pruebas o inexactas, emitidas por medios o redes de comunicación, a la correspondiente rectificación de forma inmediata. Mientras que en el otro numeral reconoce la protección de datos. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular. (Asamblea Nacional Constituyente, 2008,).

Consecuentemente la persona considerada como sujeto activo del delito de estafa mediante el uso del Deepfake en plataformas digitales, generalmente tiene conocimientos de plataforma o sistema informático. Cabe recalcar que en el COIP existe la tipificación de algunos delitos, que se aproximan, por lo cual es importante señalarlos. Así por ejemplo los constantes en los artículos 190 y 191 sobre apropiación de manera fraudulenta de sistemas informáticos o redes para estafar por medio de transferencia no consentida por la víctima; así como también tipifica la sanción de modificación o reprogramación de información en aparatos móviles.

Por otra parte, también existe sanción con pena privativa de libertad, la revelación de información registrada en archivos mediante sistema electrónico o su interceptación ilegal de datos, ejecutando transferencias electrónicas, tipificado en la sección tercera de los artículos del 229 al 231 del COIP por violar la intimidad, como un delito que es contra la seguridad, articulados que solo cuentan con una aproximación al delito de Deepfake.

## Derecho Comparado España y Estados Unidos

Es preciso mencionar que, en España, esta figura se encuentra dada para un delito en particular dentro de la “Ley de Inteligencia Artificial, por el actual avance de la innovación científica; por lo que España para estar en armonía con la Ley decretada por el Parlamento Europeo, procedió a reformar sus cuerpos legales de la Ley de Procedimiento Civil y la Ley General de Comunicación Audiovisual No 13/2022, tipificando el delito del Deepfake utilizado en estafa, suplantación de identidad, extorción, otros.

Lo dado a conocer para mejor comprensión, se muestra en el siguiente cuadro:

**Cuadro No. 1:**  
**Parlamento Europeo y España**

Parlamento Europeo	Ley de Inteligencia Artificial	<b>Artículo 3144</b> - delito de Deepfake. - es ultrafalsificación que abarca manipulación en forma de audio, vídeos o imágenes, sensación ilusoria de autenticidad y veracidad, por utilizar metodologías con inteligencia artificial.
España	Ley General de Comunicación Audiovisual No 13/2022	<b>Artículo 1:</b> Delito del Deepfake (cuando no hay autorización expresa de la persona, será delito grave).
	Ley de Procedimiento Civil	<b>Artículo 4:</b> Medida Cautelar (consiste en eliminar vídeos, voces o imágenes inventadas de personas, por sistemas automatizado, como el software al ser mecanismos actuales de la inteligencia artificial.

**Fuente:** Leyes del Deepfake en Europa. Philip Boucher, Scientific Foresight Unit (STOA). Obtenido de (Parlamento Europeo y España sobre Deepfake, 2021).

Mientras que revisando en derecho comparado en que se verifica que el Congreso de Estados Unidos resolvió decretar en el año 2018 y 2019 cuerpos legales en concreto que definieron jurídicamente el delito del Deepfake; cuyas normativas son la “Ley de Responsabilidad del Deepfake”, la “Ley de Denuncias Deepfake”; y, la “Ley de Prohibición del Deepfake”. De lo dado a conocer los cincuenta estados de United State cuentan con leyes destinadas a proteger a las víctimas del Deepfake.

## **Exposición del Problema Jurídico**

La estafa mediante el uso del DeepfaKe es un ataque de defraudación económica, donde la principal acción del sujeto activo es engañar utilizando alta tecnología para suplantar rostro y voz; por lo que según lo dado a conocer, se genera la necesidad del análisis a doctrinas y cuerpos legales como el COIP, sobre esta modalidad de estafa, reflejado en el presente documento, con la finalidad de evidenciar que en el marco ecuatoriano no existe la tipificación del delito del Deepfake, por lo cual es necesaria su incorporación dentro de la normativa vigente.

Generalmente las investigaciones del delito Deepfake se estancan por parte de los afectados, por el hecho de no cuentan con elementos de convicción adecuados para la acción penal.

La dificultad principal de seguir con las denuncias de las víctimas y la Fiscalía General del Estado como titular de la acción pública para imputar este acto delictivo mediante la dirección IP, es la difícil y compleja identificación del actor quien cometió el delito (sujeto activo), en el momento que la dirección IP no genera información suficiente para que los peritos tecnológicos de fiscalía identifiquen al responsable; esto es porque la dirección IP es generalmente propiedad de proveedores de internet del país; reiterándose que la dirección IP se utiliza para la identificación del

dispositivo (computadoras, laptop o móviles), que fueron conectados al internet, pero son aparatos que no especifican detalladamente a la persona quien estuvo utilizando aquel dispositivo.

Es importante resaltar la problemática de que no hay una normativa en que se introduzca o tipifique un artículo con las particularidades que se dan mediante Deepfake como un delito previamente en el COIP, ni método para combatir mediante un procedimiento investigativo adecuado, causando perjuicios que son para las personas irreversible y difícil de recuperar una pérdida económica.

En consecuencia, demostrar que por la falta de tipificación de este delito de Deepfake los administradores de justicia proceden a realizar una aproximación sentenciando a los sujetos activos bajo la sanción del artículo 186 del COIP.

## **PROPUESTA DE REFORMA AL COIP**

### **Considerando**

*Que artículo 1 de la Constitución, decreta el deber primordial del Estado ecuatoriano garantizar el derecho a la seguridad jurídica.*

*Que el numeral 3 del artículo 76 de la Constitución, decreta garantías constitucionales.*

*Que el inciso 26 de artículo 66 de la Constitución, decreta medidas públicas que garantizan derechos fundamentales.*

*Que el Artículo 75 de Constitución, decreta el derecho a justicia gratuita y efectiva, en concordancia con una eficaz tutela judicial efectiva.*

*Que artículo 82 de la Constitución, decreta existencia de normativas jurídicas claras y públicas.*

### **El Código Orgánico Integral Penal en el artículo 186 del delito de Estafa, textualmente señala:**

*La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.*

*La pena máxima se aplicará a la persona que:*

- 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.*
- 2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.*
- 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.*
- 4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.*
- 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.*
- 6. A través de una compañía de origen ficticio, induzca a error a otra persona, con el fin de realizar un acto que perjudique su patrimonio o el de un tercero.*

*La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.*

*La estafa cometida a través de una institución del Sistema Financiero Nacional,*

*de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos privados públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años.*

*La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad competente, será sancionada con pena privativa de libertad de treinta a noventa días.*

*Si se determina responsabilidad penal de una persona jurídica, será sancionada con multa de cien a doscientos salarios básicos unificados del trabajador en general.*

#### **Reforma en que se agregue o introduzca dentro del numeral 4 del artículo 186 de Estafa, lo siguiente:**

*La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.*

*La pena máxima se aplicará a la persona que:*

- 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.*
- 2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.*
- 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.*
- 4. Induzca a la compra o venta pública de valores por medio de actos públicos, **con el fin de obtener directa o indirectamente un beneficio económico u otro de orden material mediante el uso del DEEPFAKE, en donde colabore, ayude o participe de esta** práctica como mecanismo o artificio engañoso o fraudulento.*
- 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.*
- 6. A través de una compañía de origen ficticio, induzca a error a otra persona, con el fin de realizar un acto que perjudique su patrimonio o el de un tercero.*

*La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.*

*La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos privados públicos o de la Seguridad Social, será sancionada*

*con pena privativa de libertad de siete a diez años.*

*La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad competente, será sancionada con pena privativa de libertad de treinta a noventa días.*

*Si se determina responsabilidad penal de una persona jurídica, será sancionada con multa de cien a doscientos salarios básicos unificados del trabajador en general.*

Se debe tomar en consideración que debe existir armonía del presente tema Deepfake y reformarse también el artículo 212 del mismo cuerpo legal.

**El artículo 212 de *Suplantación de identidad*, textualmente señala:**

*La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.*

**Reforma al artículo 212 del Código Orgánico Integral Penal:**

Que se agregue o introduzca al final del artículo 212 de *Suplantación de identidad* sobre el delito de Deepfake con el siguiente contenido:

*La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.*

**La persona que, con el fin de obtener directa o indirectamente beneficio económico u otro de orden material mediante el uso del DEEPFAKE, en donde colabore, ayude o participe, será sancionada con pena privativa de libertad de tres a siete años”.**

***Justificación***

Se justifica en función a revisada la temática analizada jurídicamente con leyes del Parlamento Europeo y España, por tal razón se sugiere que se introduzca o tipifique dentro del artículo 186 y 212 al delito del Deepfake; debido a las particularidades que se dan mediante Deepfake, así se pueda sancionar y prevenir el uso indebido de este método.

## CONCLUSIONES Y RECOMENDACIONES

- La existencia del uso indebido de la tecnología cometiendo un delito de Deepfake permite abarcar múltiples campos delictivos tales como la estafa, pornografía, acoso, violencia de género, bullying, extorsión, fraudes, propagación de noticias falsas, manipulación de mercados financieros e incluso manipulación electoral.
- La seguridad jurídica es un derecho fundamental de las personas, tal como el derecho al honor y a la propia imagen, a la dignidad e intimidad personal y familiar.
- La estafa es un tipo de peligro asociado al Deepfake, por tal razón se necesita implementar medidas relevantes de inferencia probatoria epistémica para la calidad del razonamiento probatorio en delito de este delito y brindar seguridad ante la falta de regulación que es un desafío constante.
- Se recomienda que en el COIP se lleve a cabo una incorporación en el COIP para que se tipifique en un artículo el delito del Deepfake, debido a que al ser la tecnología cada vez más accesible, se amplía la posibilidad de que los ciberdelincuentes la utilicen para generar contenido malicioso utilizando el rostro y voz de otra persona y beneficiarse económicamente.

## BIBLIOGRAFÍA

- Acosta, J. (2024). *Insuficiente legislación persecutoria a delito de la estafa cibernética. Derecho Penal y Procesal Penal. Chimbote-Perú.*
- Agustino A. (2016). *Parte legal de las plataformas digitales y Deepface. Madrid. España.*
- Cornejo, J. (2023). *Delitos informáticos & Prueba en el Ámbito Penal. Santiago de Chile.* Obtenido de: [https://repositorio.uchile.cl/bitstream/handle/2250/196235/La-investigacion-de-delitos-informaticos-y-su-prueba-en-materia.](https://repositorio.uchile.cl/bitstream/handle/2250/196235/La-investigacion-de-delitos-informaticos-y-su-prueba-en-materia)
- Creismer, A. (2019). *El Comercio Electrónico en Buenos Aires. Heliasta. Argentina.* Obtenido: [http://dspace.unach.edu.ec/bitstream/51000/7607/1/8TESIS%20VER%C3%93NICA%20LILIANA%20PAGUAY%20CALDER%C3%93N-DER.pdf.](http://dspace.unach.edu.ec/bitstream/51000/7607/1/8TESIS%20VER%C3%93NICA%20LILIANA%20PAGUAY%20CALDER%C3%93N-DER.pdf)
- Gómez, J. (2022). *Identificación de sujeto activo en delito de estafa mediante plataformas digitales en Ecuador. Quito.*
- Hao, F. (2020). *Learning algorithms. Los deepfakes & ultrafalsificaciones.* Obtenido de: [https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/.](https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/)
- Iglesias, P. (2024). *Consultoría de Presencia Digital y Reputación Online. Ultrafalsificación & Deepfake. Ediciones PY. Madrid – España.*
- Oliva, L. (2022). *Deepfake con relación a la inteligencia artificial que amenaza el Derecho. Revista de Tecnología y Derecho. Lima – Perú. Págs. 79-96.*
- Pons, A. (2019) *Internet y nueva era del delito: ciberterrorismo, deepface, cibercrimen, legislación penal y ciberseguridad. Artículo de Revista Latinoamericana sobre Estudios de Seguridad. Pag. 78-101.*
- Reátegui, Sánchez (2016). *Tratado de derecho penal. Editorial San Marcos. Primera Edición. Lima – Perú .*
- Torres, C. (2020). *Breves comentarios al código penal del Ecuador. Tomo II. Volumen IV. Pág. 223 y 224.*

*Villazón, D. (2021). Delito de estafa digital. Obtenido de:  
[https://repositorio.umsa.bo/bitstream/handle/123456789/28498/TD5743.p  
df?seq.](https://repositorio.umsa.bo/bitstream/handle/123456789/28498/TD5743.pdf?seq)*

*Zavala Baquerizo (1988). Delitos contra la propiedad. Editorial Edino. Guayaquil-  
Ecuador. pág. 87.*

## DECLARACIÓN Y AUTORIZACIÓN

Yo, **Cabrera Loor, Ana Cristina**, con C.C: # 1310634249 autora del trabajo de titulación: **Delito de Estafa mediante el uso tecnológico del Deepfake** previo a la obtención del título de **Abogada** en la Universidad Católica de Santiago de Guayaquil.

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

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

Guayaquil, 20 de febrero de 2025



f. \_\_\_\_\_

Nombre: **Cabrera Loor, Ana Cristina**

C.C: 1310634249

<b>REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA</b>			
<b>FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN</b>			
<b>TEMA Y SUBTEMA:</b>	Delito de Estafa mediante el uso tecnológico del Deepfake		
<b>AUTOR(ES)</b>	Cabrera Loor, Ana Cristina		
<b>REVISOR(ES)/TUTOR(ES)</b>	Ab. Carrión Carrión, Pablo Javier, Mgs		
<b>INSTITUCIÓN:</b>	Universidad Católica de Santiago de Guayaquil		
<b>FACULTAD:</b>	Facultad de Jurisprudencia y Ciencias Sociales y Políticas		
<b>CARRERA:</b>	Derecho		
<b>TITULO OBTENIDO:</b>	Abogada		
<b>FECHA DE PUBLICACIÓN:</b>	20 de febrero del 2025	<b>No. DE PÁGINAS:</b>	21
<b>ÁREAS TEMÁTICAS:</b>	Derecho Penal.		
<b>PALABRAS CLAVES/ KEYWORDS:</b>	Estafa, Deepfake, plataformas digitales, procedimiento eficaz.		
<b>RESUMEN/ABSTRACT (150-250 palabras):</b>			
<p>Se ha llevado a cabo la elaboración del presente documento académico sobre “Delito de Estafa mediante el uso tecnológico del Deepfake”, debido al alto número de estafas transcurridas en el año 2024, utilizando el método Deepfake en plataformas digitales; ya que el problema es que en estos casos el sistema de justicia ecuatoriana lo sanciona solo como una aproximación concurrente de suplantación de identidad. Se destaca la importancia del transformar el cuerpo legal desarrollando un marco jurídico robusto dentro del Código Orgánico Integral Penal, en el cual se introduzca o tipifique un artículo de las particularidades que se dan mediante Deepfake como un delito autónomo en el COIP y así se pueda sancionar y prevenir el uso indebido de este método mediante un procedimiento eficaz del sistema de justicia.</p>			
<b>ADJUNTO PDF:</b>	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
<b>CONTACTO CON AUTOR/ES:</b>	<b>Teléfono:</b> +593-988974246	E-mail: acabrera4249@gmail.com	
<b>CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE)::</b>	Nombre: Paredes Cavero, Angela Maia .		
	Teléfono: +593 99 760 4781		
	E-mail: angela.paredes01@cu.ucsg.edu.ec		
<b>SECCIÓN PARA USO DE BIBLIOTECA</b>			
<b>Nº. DE REGISTRO (en base a datos):</b>			
<b>Nº. DE CLASIFICACIÓN:</b>			
<b>DIRECCIÓN URL (tesis en la web):</b>			