**Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas**
Año IX. Vol. IX. N° 1. Edición Especial. 2024
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela



https://doi.org/10.35381/racji.v9i1.3530

# Análisis jurídico del deepfake en relación a la suplantación de identidad, Ecuador

# Legal analysis of deepfake in relation to identity theft, Ecuador

Ronald Estiven Endara-Chamorro
dt.ronnalsec34@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Tulcán, Carchi
Ecuador
https://orcid.org/0000-0001-9240-3488

Juan Sebastián Espinoza-Jiménez
dt.juansej11@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Tulcán, Carchi
Ecuador
https://orcid.org/0000-0002-1236-0148

Eder Ronaldo López-Fuel
dt.ederrlf09@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Tulcán, Carchi
Ecuador
https://orcid.org/0009-0006-6146-7677

Jessica Johanna Santander-Moreno
ut.jessicasm33@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Tulcán, Carchi
Ecuador
https://orcid.org/0000-0001-5793-171X

Recibido: 15 de octubre 2023
Revisado: 10 de diciembre 2023
Aprobado: 15 de enero 2024
Publicado: 01 de febrero 2024

**Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas**
Año IX. Vol. IX. N° 1. Edición Especial. 2024
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela



## RESUMEN

El objetivo general de la investigación fue analizar jurídicamente el deepfake en relación a la suplantación de identidad, Ecuador. El método empleado en la investigación, se basó en el enfoque cualitativo, manejando la recolección y análisis de una tipología documental-bibliográfica. La técnica de investigación aplicada fue la entrevista. Generándose un proceso analítico–reflexivo. Se concluye que, es de suma necesidad, que, dentro del Código Orgánico Integral Penal, se incorpore un artículo enumerado, a continuación del artículo 212, dentro de los cuales se establezca el deepfake y las características en el cual procede este tipo penal, debiendo establecer la debida proporcionalidad entre la infracción cometida y el perjuicio que se está ocasionando. El avance tecnológico, está generando la aparición de nuevas modalidades de suplantación de identidad, tal es el caso de los deepfakes, los cuales ya se encuentran en el Ecuador.

**Descriptores**: Informática; identidad; derecho penal. (Tesauro UNESCO).

## ABSTRACT

The general objective of the research was to carry out a legal analysis of deepfake in relation to identity theft in Ecuador. The method used in the research was based on a qualitative approach, with the collection and analysis of a documentary-bibliographic typology. The research technique used was the interview. An analytical-reflexive process was generated. It is concluded that it is of the utmost necessity that, within the Organic Integral Penal Code, an enumerated article is incorporated, following article 212, within which the deepfake and the characteristics in which this penal type proceeds are established, establishing the due proportionality between the infraction committed and the damage that is being caused. Technological progress is generating the appearance of new forms of identity theft, such as deepfakes, which are already present in Ecuador.

**Descriptors**: Informatic; identity; criminal law. (UNESCO Thesaurus).

## INTRODUCCIÓN

El presente estudio se encuentra en el deepfake, conocido también como 'falsedades profundas', mismo que consiste en archivos de vídeo, imagen o voz, manipuladas a través de un software de inteligencia artificial, de tal manera que parezcan originales o auténticos. La capacidad de parecer reales dependerá del programa informático con el que se realice la edición; los deepfakes utilizan el aprendizaje automático de la inteligencia artificial. Esta tecnología se basa en algoritmos sofisticados que son capaces de analizar si un archivo es real o si está alterado y de esta forma, la inteligencia artificial puede ir mejorando cada vez más en la labor de falsificar de manera fidedigna. Los deepfakes pueden ser generados directamente por softwares u ordenadores especializados en este aprendizaje automático, sin necesidad de la intervención humana (LISA Institute, 2021).

Es necesario señalar que, el deepfake puede ser utilizado para la ejecución de delitos como es la suplantación de identidad, mismo que se encuentra tipificado dentro del artículo 212 del Código Orgánico Integral Penal (2014).

En la presente investigación se plantea como objetivo general analizar jurídicamente el deepfake en relación a la suplantación de identidad, Ecuador.

## MÉTODO

El método empleado en la investigación se basa en el enfoque cualitativo, manejando la recolección y análisis de una tipología documental-bibliográfica (Hernández Sampieri et al., 2014), lo cual permite organizar un análisis del objeto de estudio con la intención de descubrir el propósito presentado por los investigadores. La técnica de investigación aplicada fue la entrevista. Generándose un proceso analítico–reflexivo, contribuyendo a la generación de la extensión del estado del arte en correlación al marco jurídico científico vigente (Behar Rivero, 2018).

## RESULTADOS

La Constitución de la República del Ecuador, vigente desde el 2008 estipula lo siguiente:

> Artículo.66.- Numeral 28. El derecho a la identidad personal y colectiva, que incluye tener nombre y apellido, debidamente registrados y libremente escogidos; y conservar, desarrollar y fortalecer las características materiales e inmateriales de la identidad, tales como la nacionalidad, la procedencia familiar, las manifestaciones espirituales, culturales, religiosas, lingüísticas, políticas y sociales.

Esta disposición señala el derecho a una identidad, el cual no solo comprende tener un nombre y apellido, sino también una identidad como personas tomando en cuenta sus características físicas como su rostro o color de piel; en este sentido, resulta importante realizar el presente estudio debido a que se ha convertido en un problema común, que con el avance de la tecnología, fácilmente se pueda suplantar la identidad de otras personas, tan solo para jugarle una broma, dañar su reputación o el peor escenario para cometer actos fraudulentos.

Por otro lado, con respecto al problema, el Código Orgánico Integral Penal (2014) señala:

> Artículo. 212.- Suplantación de identidad. -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.

Del análisis de esta disposición, si bien, por un lado, señala a la persona que de cualquier forma suplante la identidad, en sentido general, incluye a la suplantación de identidad digital, más, sin embargo, al ser un delito de resultado, se requiere el resultado material o ideal, consecuencia de la conducta ilícita. Bajo este contexto, en la actualidad, el avance informático ha permitido la creación del deepfake, conocido también como falsedades profundas, y constituyen videos, imágenes o voz que han sido manipuladas mediante software de inteligencia artificial de tal modo que parecen reales; sobre ello existe variedad de preocupaciones en torno a la solución de los problemas que ha

estado causando el uso malicioso del deepfake, pues, en su mayoría, colocan la atención en el componente tecnológico, lo cual no se alude; no obstante, la gravedad del problema requiere, no sólo soluciones tecnológicas, sino también integrales, multifacéticas y legales con un enfoque antropocéntrico, que regule el comportamiento moral desde la perspectiva legal, asegurando coherencia social, en lo que debe prevalecer un sistema de valores, normas, principios e ideales que guían el proceder de los individuos en la sociedad. En este entorno, en el debate de enfrentamiento al deepfake, frente a las normas jurídicas, se observa lentitud en el marco legal con relación al desarrollo tecnológico, además, esta modalidad de suplantación es en el área pornográfica, o para generar desinformación.

Un estudio sobre deepfake: “Inteligencia artificial y algoritmo que causa riesgos a la sociedad en el ciberespacio” establece que la inteligencia artificial utilizada en los deepfakes actúa directamente sobre la desinformación global, reproduciendo información falsa, engañosa, fuera de contexto y diseñada para dañar la colectividad, provocando un colapso de desconfianza hacia todo lo que se publica en la red mundo de las computadoras, un hecho que requiere que los internautas comprueben sobre la veracidad de la información recibida. Está claro que las redes sociales digitales influyen directamente en el comportamiento humano, por lo que es necesario pensar sobre la importancia de verificar los hechos antes de compartirlos con toda la red de amigos digitales, siendo este el primer paso para enfrentar la desinformación proporcionados por herramientas de inteligencia artificial. ‘Es responsabilidad del ser humano la protección de los principios fundamentales de manera plural, democrática e interconectada (Robles, 2020).

Otra investigación sobre deepfake: “Una base de datos de trastornos faciales humanos”, señala que la cara es una parte integral del cuerpo humano por la cual un individuo se comunica en la sociedad. Su importancia puede ser destacada por el hecho de que una persona privada de rostro no puede sostenerse en el mundo de los vivos. En las últimas décadas, el rostro humano ha llamado la atención de varios investigadores, ya sea

relacionado con la antropometría facial, el trastorno facial, el trasplante o la reconstrucción facial. Sin embargo, en la actualidad, no existe tal base de datos que proporcione no solo imágenes faciales de individuos; sino también la literatura sobre el rostro humano, lista de varios genes que controlan el rostro humano, lista de trastornos y diversas herramientas que trabajan sobre imágenes faciales.

Por lo tanto, la investigación actual tiene como objetivo desarrollar una base de datos de trastornos faciales utilizando el enfoque bioinformático. La base de datos contendrá información sobre enfermedades faciales, medicamentos, síntomas, hallazgos, etc. Inicialmente, las enfermedades específicas del rostro humano han sido obtenidas de corpus de literatura publicados y creados utilizando el enfoque de minería de texto. Se creará un conjunto de datos y se almacenará en forma de base de datos. Será una base de datos que contenga un índice de referencias cruzadas de enfermedades faciales humanas, medicamentos, síntomas, signos, etc. Así, una base de datos sobre el rostro humano con la información existente completa sobre los trastornos faciales humanos se desarrollará. La novedad de la base de datos radica en que es la primera de su tipo. (Kaur, 2017).

En este orden de ideas, los deepfakes son vídeos en los que el rostro y la voz de una persona que, de manera habitual son figuras públicas, han sido manipulados utilizando un software de inteligencia artificial que permite que estos hagan y digan cosas distintas a las que contenía el video original, logrando así obtener vídeos hiperrealistas generando la sensación de que el video que han creado es auténtico (Azuaje Pirela, 2021).

Es evidente que este avance tecnológico puede ser usado indistintamente, más, sin embargo, desde la esfera del derecho, deben establecerse los límites que permitan regularlo en las normas penales. La técnica permite crear vídeos hiper falsos, también denominados videos ultra falsos, por medio de la edición automática de imágenes y sonidos que desarrolla la inteligencia artificial a través del Deep Learning. El objetivo de tales videos es entonces poder realizar copias digitalizadas de cualquier personaje

público o privado para poder hacer que esta copia haga o diga lo que el autor o autores de esta creación se les ocurra (Lavanda, 2022)

Al respecto, la inteligencia artificial se encuentra en pleno auge, algunos hablan de una nueva revolución que podría cambiar la vida en nuestro planeta de manera radical, como lo es la inteligencia artificial, misma que afecta a todos los aspectos de la vida, trabajo, movilidad, medicina, economía o comunicación, en casos como mejorando la medicina y sustituyendo al médico, la llegada de los robots inteligentes que se harán cargo de nuestros trabajos, entre otros aspectos que permitirán determinar qué es lo que puede hacer realmente, que cambiará y qué será pura utopía.

Hay que tener presente que un computador analiza la información por datos, es así como el rostro es un conjunto de datos mínimos que permiten reconstruir la expresión, posición y gestos de un rostro (Torres, 2019). Por lo general, en el Deepfake mediante la inteligencia artificial, los videos son manipulados en los rostros de los participantes cambiándose con rostros de otras personas, en los que se maneja no solo sus movimientos, sino también sus palabras, voz y gestos, a tal punto de que a simple vista pasan por auténticos. Para lograr la reconstrucción o cambio del rostro, se necesita de tres etapas, las cuales son:

1. Extracción de la imagen (rostro)
2. Procesamiento del rostro falso
3. Inserción de una máscara dentro del fotograma.

Una de las principales consecuencias de los deepfakes, y que ha generado gran connotación para algunos expertos es la utilización de sistemas biométricos, es decir, que al poderse sustituir y rostro de cualquier persona y podría acceder a sistemas restringidos.” De las que se puede citar la utilización de cebo-de-clics (clicbait) que combinado con ingeniería social se obtendría información personal de la víctima para un posterior robo o coacción (Stupp, 2019). Alertar sobre estos peligros no es aumentar la alarma sobre el deepfake o alentar una campaña para prohibir su estudio académico. Más bien de regular su utilización en la esfera pública, crear conciencia en la población y

mostrar varias facetas que los profesionales del Derecho deben considerar: atribuciones por copyright, de identidad digital, preservación del buen nombre, relaciones internacionales, entre otras. Prevenir el mal uso de esta herramienta es el primer paso para que la desinformación (un tipo de engaño premeditado) conlleve a efectos indeseables tanto sociales como económicos (Torres, 2019).

En cuanto a la suplantación de identidad, la Constitución de la República del Ecuador (2008), dentro de su artículo 66, numeral 28 señala, el derecho a la identidad personal y colectiva, esta disposición engloba el derecho a una identidad, el cual no solo comprende tener un nombre y apellido, sino también una identidad como personas tomando en cuenta sus características físicas como su rostro o color de piel; en este sentido, debido a los avances tecnológicos resulta fácil suplantar la identidad de otras personas, tan solo para jugarle una broma, dañar su reputación o el peor escenario para cometer actos fraudulentos.

Se puede precisar que el sujeto activo es atribuible a cualquier persona que posea habilidades sobre el dominio de sistemas informáticos, ya que la parte ofendida o sujeto activo es una persona natural. La suplantación de identidad puede calificarse como un delito de resultado (Zorrilla, 2018).

## DISCUSIÓN

La utilización de los deepfakes dentro de la sociedad, generan gran afectación en las personas. ya que además de afectar el derecho al buen nombre, atacan la honra y reputación de las personas; no obstante, tiene gran incidencia con el delito de suplantación de identidad debido a que el deepfake constituye una herramienta tecnológica que permite cambiar de rostro a una persona dentro de un video, imagen o voz, de tal manera que hace presumir que el video que se ha creado puede ser fácilmente pasado como auténtico y real.

En este aspecto el delito de suplantación de identidad contemplado dentro del artículo 212 del COIP (2014), de manera generalizada establece que 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. Es claro que esta disposición no dice nada respecto a la suplantación que se realiza a través del deepfake, razón por la cual, es imperante determinar cómo se debería regular este delito informático.

Dentro de la normativa penal no se encuentra establecido el delito de deepfake, el cual debería consistir en que la persona que realice mediante tecnologías informáticas o inteligencia artificial la suplantación de identidad de una persona natural, con algún beneficio y cause perjuicio a otra, de manera material, se pondrá una pena dependiendo del perjuicio ocasionado, en igual forma se deberá tener presente si el deepfake ha sido creado con la finalidad de ejercer violencia material o psicológica sobre una persona; o para desinformar, o generar actos de manipulación con determinada persona.

## CONCLUSIONES

Se concluye que es de suma necesidad, que, dentro del Código Orgánico Integral Penal, se incorpore un artículo enumerado, a continuación del artículo 212, dentro de los cuales se establezca el deepfake y las características en el cual procede este tipo penal, debiendo establecer la debida proporcionalidad entre la infracción cometida y el perjuicio que se está ocasionando. El avance tecnológico, está generando la aparición de nuevas modalidades de suplantación de identidad, tal es el caso de los deepfakes, los cuales ya se encuentran en el Ecuador y que han sido utilizados con fines de concientización; sin embargo, ante la llegada de esta tecnología en nuestro país, se deja abierta la posibilidad de cometer actos delictivos, situación que el legislador no ha previsto.

## FINANCIAMIENTO

No monetario.

## AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes, Sede Tulcán, por motivar el desarrollo de la Investigación.

## REFERENCIAS CONSULTADAS

Asamblea Nacional (2014). Código Orgánico Integral Penal. [Comprehensive Criminal Code]. Registro Oficial Nº 180. https://url2.cl/53c6h

Asamblea Nacional Constituyente de la República del Ecuador (2008). Constitución de la República del Ecuador. [Constitution of the Republic of Ecuador]. Montecristi. Registro Oficial 449 de 20-oct-2008. https://n9.cl/i1ch

Azuaje, M. (2021). Deepfake Mom: Desafíos tecnológicos Derecho. [Deepfake Mom: Technological Challenges]. Estado Diario. https://n9.cl/1ezlc

Behar Rivero, D. (2018). Metodología de la Investigación. [Investigation methodology]. https://n9.cl/k9q2

Hernández, R., Fernández, C., y Baptista, M. (2014). Metodología de la Investigación [Investigation Methodology] (5ta. ed.). México: McGraw-Hill.

Kaur, P. (2017). DisFace: A Database of Human Facial Disorders. https://doi.org/10.24870/cjb.2017- a12

Lavanda, M. (2022). Deepfake: Cuando la inteligencia artificial amenaza el Derecho y la Democracia. [Deepfake: When Artificial Intelligence Threatens Law and Democracy]. *Lawgic Tec - Revista de Derecho y Tecnología,* 2(1). https://n9.cl/kuwcj

LISA Institute (2021). Deepfakes: Qué son, tipos, consejos, riesgos y amenazas. [Deepfakes: What are they, types, tips, risks and threats]. https://n9.cl/57gfw

Robles, M. (2020). Deepfake: inteligencia artificial y algoritmo que causa riesgos a la sociedad en el ciberespacio. [Deepfake: artificial intelligence and algorithm causing risks to society in cyberspace]. *Derecho y cambio social*, 61, 475-487. https://n9.cl/mnm3v

Stupp, C. (2019). Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. The Wall Street Journal. https://n9.cl/id3gm

Torres, V. (2019). Tendencias de videos ultrafalsos para profesionales del derecho. [Ultra-fake video trends for legal professionals]. https://n9.cl/7h0go

Zorrilla, K. (2018). Inconsistencias y Ambigüedades en la Ley de Delitos Informáticos Ley Nº 30096 y su Modificatoria Ley Nº 30171, Que Imposibilitan su eficaz Cumplimiento. [Inconsistencies and Ambiguities in the Law on Computer Crimes Law Nº 30096 and its Amending Law Nº 30171, which hinder its effective enforcement]. Tesis de Pregrado. Universidad Nacional de Ancash. https://n9.cl/6dyqr