UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TEMA:

Suplantación de identidad mediante el uso de IA

AUTORES

Casquete Correa, Wendy Solange

Yépez Frugone, Doménica Fabiola

Trabajo de titulación previo a la obtención del título de ABOGADA

TUTOR:

Abg. Cuadros Añazco, Xavier Paul Mgs.

Guayaquil, Ecuador

25 de agosto del 2026

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Casquete Correa Wendy Solange** y **Yépez Frugone Doménica Fabiola**, como requerimiento para la obtención del título de **Abogada.**

TUTOR (A)

Xavier Paul Cuadros Anazco
Time Stamping Security Data

f. _____

Abg. Cuadros Añazco, Xavier Paul Mgs.

DIRECTOR DE LA CARRERA

f. _____

Dra. Nuria Pérez Puig-Mir, PhD.

Guayaquil, a los veinticinco días del mes de agosto del año 2026

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS
CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotras, **Casquete Correa Wendy Solange; Yépez Frugone Doménica Fabiola**

DECLARAMOS QUE:

El Trabajo de Titulación, **Suplantación de identidad mediante el uso de IA**, previo a la obtención del título de **Abogada** ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de nuestra total autoría.

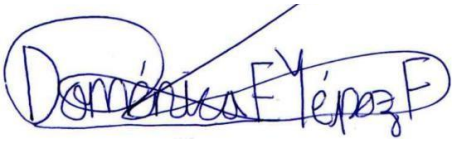
En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 25 días del mes de agosto del año 2026

AUTORAS

f. 

Casquete Correa Wendy Solange

f. 

Yépez Frugone Doménica Fabiola

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS
CARRERA DE DERECHO

AUTORIZACIÓN

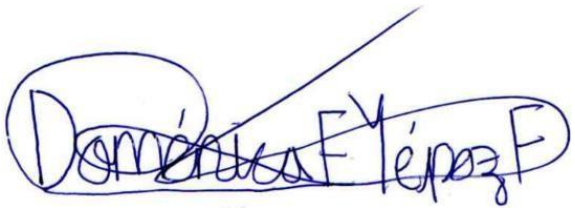
Nosotras, **Casquete Correa Wendy Solange;**
Yépez Frugone Doménica Fabiola

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Suplantación de identidad mediante el uso de IA**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 25 días del mes de agosto del año 2026

AUTORAS

f. 
Casquete Correa Wendy Solange

f. 
Yépez Frugone Doménica Fabiola

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS
CARRERA DE DERECHO

REPORTE COPILATIO


Certificado de análisis
Compilatio Magister+ | UCSG-EC- Universidad Católica de Santiago de Guayaquil

Tesis final
ID : 1f161b1dba3f6f8c1db63ff81652fb8f4562fefc

5%
Textos sospechosos

Nombre del fichero : Tesis final.txt
Tamaño del archivo original : 402,4 kB
Número de palabras : 11.405

Depositante : xXavier Paul Cuadros Añazco
Fecha de depósito : 20 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 20 de agosto de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

TUTOR

Xavier Paul Cuadros Anazco
Time Stamping Security Data

f. _____

Abg. Cuadros Añazco, Xavier Paul Mgs.

AUTORAS

f. Wendy Casquete C

Casquete Correa Wendy Solange

f. Doménica F Yépez F

Yépez Frugone Doménica Fabiola

Agradecimientos

Agradecimiento de Wendy Solange Casquete Correa

Agradezco a Dios y a mi Madre del Cielo por sus infinitas bondades y por permitirme comprender que los obstáculos también se convierten en bendiciones.

A mis padres, y abuelita materna, por ser mis mejores guías en la vida.

A mis hermanos, María Auxiliadora y Michael, gracias por acompañarme en mis tristezas y alegrías, por creer en mí y, sobre todo, por regalarme la dicha de poder soñar como una niña junto a ustedes. Son mi mejor regalo e inspiración.

A mi compañera y amiga de tesis, Doménica Yépez, por la paciencia y el cariño que me ha regalado en este camino.

A los amigos que hice durante la carrera, en especial a Danna y Samuel, por su cariño y por ser compañía en mis momentos de incertidumbres.

A mi familia en general y a todos quienes, de algún modo, creyeron en mí. ¡Infinitas gracias!

Agradecimiento de Doménica Fabiola Yépez Frugone

Primeramente, le agradezco a Dios quien es mi fortaleza y me ha permitido tener la oportunidad de vivir plenamente y estar el día de hoy.

También le doy las gracias a mis padres quienes son mi apoyo tanto emocional como económico, y por ellos soy quien soy hoy en día, son el pilar de mi vida. A mi familia tanto materna como paterna, con quienes sé que podré contar.

A mi abuelita, quien se encuentra en el cielo, pero sé que me cuida y está orgullosa de mí por este gran momento de mi vida.

A mis amigos y compañeros de la facultad con quienes me conozco desde el primer semestre de esta grata experiencia y ha sido un largo y emocionante camino junto a ellos.

A mis profesores, quienes me han guiado profesionalmente en esta trayectoria académica en mi Alma Mater, la UCSG. Y finalmente, gracias a mi compañera Wendy Casquete, con quien tengo la dicha de decir que nos conocemos desde aquel lejano año 2022, y hoy en día más que ser una compañera de tesis, es mi gran amiga con quien pude compartir este trabajo que significa mucho para ambas.

Dedicatorias

Dedicatoria de Wendy Solange Casquete Correa

Dedico este trabajo de titulación a mis padres, quienes sembraron en mi corazón el deseo inquebrantable de hacer siempre el bien.

De manera especial a mi madre, Rocío Correa, columna vertebral de todos mis sueños, quien me lo ha dado todo sin medir condiciones y que, sobre todo, me ha enseñado a mirar el cielo con fe y esperanza.

A la memoria de mi padre, Francisco Casquete, porque, aunque sus brazos ya no me abracen físicamente y sus ojos no se posen sobre estas líneas, continúa siendo mi mayor apoyo y la inspiración que guía cada uno de mis pasos.

Asimismo, a mi abuelita, Dolores Herrera, quien, sin haberme llevado en su vientre, me amó y cuidó con la ternura más pura, dejando en mí su fortaleza, aquella que hoy me acompaña al transitar por la vida.

Dedicatoria de Doménica Fabiola Yépez Frugone

Este trabajo se lo dedico primeramente a Dios que ha estado conmigo permitiéndome estar con fuerza en este preciso momento.

También se la dedico a mi abuelita, que en paz descanse, quien desde el cielo me está viendo graduándome de abogada.

Se la dedico a mis padres quienes han sido mi apoyo y acompañamiento emocional constante en estos 4 años y medio de carrera universitaria.

Y finalmente, me la dedico a mí misma y a mi amiga y compañera Wendy Casquete, porque solo nosotras sabemos el exhaustivo esfuerzo que nos ha tomado llegar hasta donde estamos el día de hoy.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS
CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

Dr. LEOPOLDO XAVIER ZAVALA EGAS
DECANO DE CARRERA

f. _____

Ab. MARITZA GINETTE REYNOSO GAUTE, Mgs.
COORDINADOR DEL ÁREA

f. _____

Dr. JOSÉ MIGUEL GARCÍA AUZ
OPONENTE

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: **Jurisprudencia**
Carrera: **Derecho**
Periodo: **Semestre A - 2026**
Fecha: **24 de agosto 2026**

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado ***SUPLANTACIÓN DE IDENTIDAD MEDIANTE EL USO DE IA*** elaborado por las estudiantes ***DOMÉNICA FABIOLA YÉPEZ FRUGONE y WENDY SOLANGE CASQUETE CORREA,*** certifica que durante el proceso de acompañamiento dichos estudiantes han obtenido la calificación de ***10 (DIEZ),*** lo cual los califica como ***APTAS PARA LA SUSTENTACIÓN.***

Xavier Paul Cuadros Anazco
Time Stamping Security Data

ABG. MGS. XAVIER CUADROS AÑAZCO

Índice

Resumen

La Inteligencia Artificial es una herramienta útil en el ámbito laboral, jurídico o académico, pero es un arma de doble filo si no se implementa con regulación y control para evitar su uso malicioso. El eje central de este análisis es la suplantación de identidad por medio de la IA; un problema actual ya que el Código Orgánico Integral Penal (COIP) no regula estos delitos ni el almacenamiento masivo de datos biométricos. Por lo cual, existe una enorme dificultad para identificar responsables en modalidades como *deepfakes*. Al utilizar medios ilícitos para robar datos personales de un individuo o figura pública, se busca suplantar su identidad creando clones digitales de su voz o imagen, facilitado por la complejidad algorítmica y la falta de sanciones. Ante esta situación, nuestra idea es proponer un conjunto de normas y sanciones claras para quienes incumplen la ley. Por otro lado, queremos sembrar el uso de tecnologías transparentes, y ayudar a que los individuos comprendan de mejor manera el mundo digital actual. Para alcanzar ese objetivo, hemos estudiado leyes de diferentes países de Latinoamérica y la Unión Europea que ya trabajan en el tema en cuestión. Después del análisis profundo de los diferentes acuerdos internacionales que Ecuador ha firmado, creemos conveniente modificar el artículo 212 del COIP, para de esa manera, evitar confusiones e interpretaciones erróneas.

Palabras clave: *Titular, datos personales, identidad, inteligencia artificial, ciberseguridad, informática.*

Abstract

Artificial Intelligence is a useful tool in the workplace, legal, and academic fields, but it is a double-edged sword if implemented without regulation and control to prevent malicious use. The central focus of this analysis is identity theft through AI; a current problem since the Organic Integral Criminal Code (COIP) does not regulate these offenses or the mass storage of biometric data. Consequently, there is an enormous difficulty in identifying those responsible for methods such as deepfakes. By using illicit means to steal personal data from an individual or public figure, attackers seek to impersonate them by creating digital clones of their voice or image, a process facilitated by algorithmic complexity and a lack of sanctions. In response, we propose regulatory frameworks with specific penalties, transparent technologies, and digital literacy, especially for digital forensic experts. This is based on comparative legislation from countries in Latin America and the European Union. After analyzing international treaties to which Ecuador is a party, we consider it necessary to modify and expand Article 212 of the COIP to avoid ambiguous interpretations.

Key words: *Owner, personal data, identity, artificial intelligence, cybersecurity, information technology.*

Introducción

La actual era digital ha tenido un impacto significativo en nuestra vida cotidiana, más precisamente en la creación y uso de nuevas herramientas que antes no existían, entre ellas, la Inteligencia Artificial (IA). Si bien, la IA es de gran utilidad hoy en día para la elaboración de diversas actividades en distintos campos, como el laboral o el académico, no es menos cierto que al mismo tiempo también es necesario entender hasta qué punto esta es una herramienta y cuando se convierte en un obstáculo para las personas en general. El acelerado avance de la IA presenta una infinidad de retos sustanciales al presentarse dentro de diversos contextos de nuestra cotidianidad, entre estos está el ámbito jurídico y legal al existir un uso no concedido e indebido de imágenes, información y datos personales de un individuo sin que éste lo haya solicitado o permitido, lo cual constituye en una acción penal. Un ejemplo de ello, es el Caso 700 IA en Ecuador que se lo analiza en el artículo de (Mejía Terán, 2025), en donde una diversidad de imágenes de jóvenes fue manipulada sin su previo consentimiento con el fin de generación de contenido pornográfico creado mediante el uso de Inteligencia Artificial, ello evidencia una clara ausencia de marcos normativos claros para poder proteger a las personas contra tales vulneraciones a sus derechos. Por todo lo antes mencionado, es sumamente necesario analizar el alcance del artículo 212 del COIP y determinar si su regulación resulta suficiente para proteger el derecho a la identidad y responder eficazmente a las conductas ejecutadas mediante IA.

Capítulo I

1. Antecedente Histórico Jurídico

Los orígenes de la Inteligencia Internacional datan del año 1936, cuando el matemático y científico computacional Alan Turing desarrolló el concepto de los números computables, cimiento de los modelos matemáticos de redes neuronales propuestos por los neurocientíficos. Posteriormente, fueron Warren McCulloch y Walter Pitts en el año 1943 quienes presentaron un modelo matemático de neuronas artificiales, ello fue considerado como uno de los primeros prototipos desarrollados de la IA. Durante los años siguientes, hubo un avance significativo en algoritmos y programas para imitar las capacidades y el raciocinio humano para la resolución de problemas.

Siendo que, por ejemplo, Alan Turing en su artículo *Computing Machinery and Intelligence*, introduce el conocido Test de Turing o juego de la imitación para evaluar si una máquina puede mostrar comportamiento e inteligencia similar a la de un ser humano con el cual buscaba responder a la pregunta: ¿las máquinas pueden pensar? (Turing, 1950). Durante la conferencia de Dartmouth en 1956 se acuñó formalmente el término de IA, puesto que Jhon McCarthy, Marvin Minsky, Claude Shannon y otros grandes ponentes definieron la IA como la ingeniería y ciencia para crear máquinas inteligentes, marcando así un comienzo oficial de dicha área. También se destaca el proyecto *General Problem Solem* de 1957, creado por Allen Newell, Herbet Simon y J.C. Shaw para el desglose de problemas y soluciones fácticas.

Sin embargo, no es sino hasta la década de 1980 que, gracias a las computadoras personales y al Internet que la IA ha podido mostrar su auténtico potencial. Ambas tecnologías han establecido y consolidado el sector de las telecomunicaciones mediante los teléfonos inteligentes, extendiendo su utilización a cientos de millones de usuarios en los primeros diez años del siglo

XXI. Todo portador de un Smartphone se convirtió en usuario indirecto o directo de la IA en la década del 2010, cuando bajo la justificación de personalizar las experiencias, se integra para detectar patrones de consumo de los usuarios, así lo mencionan (Bonilla Yoza et al., 2022): *Hasta hace algún tiempo, la IA estaba reservada para los equipos más costosos, los de gama alta, que utilizaban la tecnología más avanzada. Pero los fabricantes de procesadores y de componentes se han preocupado por llevar a la gama medias funciones avanzadas por precios más asequibles. La inteligencia artificial (IA) está tomando cada vez más peso en todo lo que nos rodea. Gran parte de la importancia que va ganando esta tecnología viene provocada por el auge del uso de los asistentes virtuales. Las personas cada vez van confiando más en estos dispositivos y los utilizan en su día a día*.

La inteligencia artificial, que más adelante nos referimos como IA, ha sufrido una expansión exponencial, lo cual ha transformado diferentes campos. No obstante, su utilización por parte de los usuarios sin conciencia y sin las regulaciones apropiadas genera, entre otros peligros, la alteración de la realidad. Por lo tanto, se ha notado en la actualidad un aumento de los casos de suplantación de identidad a través de IA, un crimen que ha ido en ascenso en las décadas recientes y que en delitos informáticos ha sido muy utilizado en estos últimos años por los cibercriminales. Este crimen se basa, fundamentalmente, en la apropiación indebida de una identidad. digital de un individuo para conseguir datos personales y, de esa manera, tener acceso a llevar a cabo varias conductas, algunas de las cuales son constitutivas de otros tipos penales que pueden variar desde la afectación de bienes patrimoniales y económicos, así como daños a bienes jurídicos que estén protegidos como el honor, la identidad y la reputación.

Se reconoce que la IA es el proceso que permite a las máquinas emular las redes neuronales humanas y artificiales (naturales e ideales), logrando automatizar proceso y

comprender lenguajes, abstraer conceptos, procesar grandes cantidades de información, resolviendo de esta forma problemas complejos en tiempo récord, más allá de las capacidades previstas. La IA se nutre de la interacción con sus usuarios, creando redes de conocimiento capaces de reemplazar la identidad humana. Uno de los riesgos más grandes es que la realidad sea distorsionada y no se pueda distinguir entre una *deepfake* y lo verdadero. La falta de políticas que definan los controles y regulaciones para la implementación de la IA, así como la ausencia de responsabilidad individual en su uso, son áreas que requieren atención urgente.

2. Conceptos – nociones

2.1. Suplantación De Identidad

La suplantación de identidad se puede interpretar de manera gramatical desde los términos literales que componen dicha expresión, es así como la suplantación, según el diccionario de la RAE, es la acción o efecto de suplantar, término que proviene del latín *supplantāre* que significa derribar y consiste en ocupar el lugar de alguien más, de manera deshonesta para aprovecharse de la situación y perjudicarla. Por otro lado, según la (RAE, 2024) el término identidad proviene del latín identĭtas y significa,"Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás". En las redes sociales, la suplantación de identidad es una forma de fraude en línea que ocurre cuando los delincuentes se hacen pasar por alguien más, ya sea creando un perfil falso o asumiendo el control de una cuenta preexistente. Así como nos lo menciona (García Merino, 2024): *La IA se alimenta de la interacción con sus usuarios, generando redes de conocimiento capaces de suplantar la identidad humana, siendo uno de los mayores riesgos la distorsión de la realidad donde no se distinga entre una deepfake (contenido falso y realista).* Esto se hace normalmente con la finalidad de que los individuos divulguen información personal, participen en actividades fraudulentas o puedan calumniar a la

persona en cuestión. Los defraudadores, en la mayoría de las ocasiones, se hacen pasar por individuos de confianza, como parientes, amigos o personajes públicos conocidos, con el fin de obtener la confianza de quienes son sus víctimas. No obstante, cualquier individuo, sin importar el grado de popularidad que tenga en las redes sociales, puede ser víctima de la suplantación de identidad.

2.2. Bien jurídico protegido

La figura del bien jurídico protegido corresponde al derecho que la ley reconoce como merecedor de protección contra conductas que puedan afectar este derecho. Dicha protección, para el caso concreto del delito de suplantación de identidad, se encuentra sujeta a la protección del derecho a la identidad. Dicho derecho a la identidad se puede considerar constituido por aquellos elementos que permitan reconocer y diferenciar a una persona entre las demás.

Ello está ejemplificado como nos lo menciona (Martínez Galindo, 2024): *En el caso de la nueva tecnología, la identidad de una persona no se puede reducir solo al simple nombre o apellidos que una persona está identificada, sino también y si no es más, por todos aquellos datos o elementos que representen a una persona dentro del escenario virtual, entre los cuales se encuentran los datos personales, su lugar de vivienda, correo electrónico, teléfono, perfiles o usuarios en las redes sociales, fotografías, imagen personal, información de su navegador, entre otros datos o información relacionados con la persona.*

Por tal razón, resulta que las nuevas tecnologías y su desarrollo, hacen que la identidad tenga también un componente digital y que su protección tenga importancia también en la esfera

digital, así como otros aspectos, intimidad, privacidad, libertad individual, que se verán afectados. Es en este sentido que el artículo 212 del Código Orgánico Integral Penal protege de forma directa la identidad de la persona, ante aquellos actos de suplantación por medio de los cuales una persona lleva a cabo actos para poner en riesgo o afectar su identidad para, de alguna manera, obtener un beneficio para sí o para una tercera persona o terceras personas, en contraste con el interés de otra persona. Frente a las nuevas modalidades tecnológicas del delito de suplantación de identidad que surgen, es necesario evaluar si el bien jurídico protegido de la persona se ve suficientemente protegido, tanto en su dirección como de cualquier otra finalidad.

2.3. Datos Personales

La suplantación de identidad tiene una enorme relación con los datos personales junto con su protección jurídica. Estos son comprendidos como cualquier dato o información que identifique a una persona natural por quién es y la diferencie de otros individuos, además de que implica de información confidencial que debe ser respaldada. El derecho de identidad de una persona es irrenunciable en sí mismo al igual que otros derechos, este es irrenunciable respecto a sus datos, y lo que implica con estos, como lo son la rectificación, acceso, oposición, portabilidad y eliminación. Se relaciona además con el derecho de confidencialidad, el cual incluye el acceso, control y decisión sobre sus propios datos personales para de dicha manera se pueda regular su tratamiento, almacenamiento y difusión, tras la autorización del titular mediante mandato legal o permiso directo constatado dentro de un documento escrito, salvo los casos exceptuados por la ley. Esta información se encuentra regulada dentro de nuestra legislación por la Ley Orgánica de Protección de Datos, cuyo objetivo principal es el garantizar que los datos personales sean tratados respecto a los principios de transparencia y proporcionalidad, junto con los deberes, obligaciones,

con mecanismos legales correspondientes para corregir y sancionar las vulneraciones que se presenten, y que así se pueda asegurar que la información personal se permita que sea manejada de una manera segura, transparente y bajo control del titular.

Un caso internacional relacionado a la protección de datos es la sentencia de La Haya con fecha del 5 de febrero del 2020, en la cual, según (van Veen, 2020), se trata de la primera sentencia europea que declaró ilegal un algoritmo de evaluación de características personales de los ciudadanos por no ser clara ni verificable. En este fallo histórico, el Gobierno de Países Bajos utilizó algoritmos de IA para identificar unos supuestos fraudes en seguridad social y contribuciones fiscales. Ese sistema analizaba los datos personales de forma automatizada para detectar patrones que podrían tratarse de fraude.

Sin embargo, las personas afectadas no tenían acceso ni claridad sobre cuáles eran los criterios que el sistema utilizaba para afirmar que se trataban de sospechosas o no, ni sabían cómo era el funcionamiento del algoritmo al sustraer sus datos personales. Se determinó que dicho sistema no cumplía con los requisitos legales correspondientes de proporcionalidad, transparencia y respeto a la privacidad, violando así el Convenio Europeo de Derechos Humanos. Por lo tanto, este caso es considerablemente impactante como un precedente para la protección importante dentro del ámbito de la regulación de tecnologías algorítmicas y protección de los derechos digitales, lo cual obliga a los gobiernos a ser más plausibles y cuidadosos cuando hacen uso de la inteligencia artificial en ámbitos de seguridad jurídica.

2.4. Falsedad informática

Según el Código Orgánico Integral Penal, en el Art. 234.1., el delito de falsificación informática consiste en la manipulación, creación, modificación o alteración fraudulenta de datos, programas, sistemas, documentos que reposan en contenido digital o informático con el objetivo de generar un daño o perjuicio al producir información falsificada o no auténtica y que pueda pasar como fidedigna. La IA se encuentra estrechamente vinculada a este delito debido a que los actores del mismo utilizan la IA para el robo de documentos y datos digitales para así generar perfiles electrónicos manipulados y documentos falsos o modificados ilícitamente, puesto que así los delincuentes se hacen pasar por la identidad de otra persona.

3. Elementos

En varios países alrededor del mundo ya se ha hecho presente la incorporación de marcos legales específicos los cuales se encargan de regular y controlar el uso de la Inteligencia Artificial, con el fin de que sea ético, transparente y seguro. Estas normativas promueven aspectos tales como la seguridad personal, la privacidad de datos, la rendición de cuentas y la prevención de sesgos algorítmicos. En consideración de ello, es necesario que dentro de la legislación ecuatoriana se adopten y adapten los modelos pertenecientes a otras naciones para así, al seguir dicho ejemplo pueda ser regulado el uso de IA en nuestro medio y poder determinar las sanciones correspondientes. Tal como nos lo dice (Maldonado Montenegro, 2025), se debe realizar un análisis exhaustivo sobre cómo agregar una tipificación de los delitos cibernéticos hechos con IA.

Algunos de los elementos fundamentales pertenecientes a las normativas de otros países que deberían ser incluidos dentro de la legislación ecuatoriana son los siguientes: La protección de datos personales, promoción de un desarrollo tecnológico ético y sustentable, la responsabilidad

civil y penal, protocolos de transparencia y auditoría, y estándares técnicos de seguridad. Entre las legislaciones extranjeras en las cuales el Estado Ecuatoriano se puede basar para la implementación de una protección más firme respecto a los datos personales e imagen con el uso de IA, son las siguientes:

Primero, la (Ley que modifica el Código Penal, Decreto Legislativo 635, y la ley 30096, Ley de delitos informáticos, para incluir el uso de la Inteligencia Artificial en la comisión de delitos, 2025) de la República del Perú, siendo esta una ley la cual modifica su Código Penal mediante el decreto legislativo 635 y la Ley de Delitos Informáticos 30096 para incluir el uso de la inteligencia artificial para la comisión de delitos. Esta presente ley introduce expresamente el uso indebido de tecnologías basadas en inteligencia artificial como una herramienta, cuyo objetivo es actualizar el marco jurídico regulatorio adaptándose a la era actual donde se ve la necesidad de regular una nueva modalidad de delitos dentro del aspecto cibernético, es decir, una ampliación de esta sección de delitos dentro de su Código Penal. A lo cual, es necesario seguir y basarse en dicho ejemplo para poder realizar una modificación oportuna y adaptarlo al Código Orgánico Integral Penal ecuatoriano, estableciendo penas de libertad más severas cuando la suplantación de identidad para el cometimiento del delito de estafa se realiza mediante la manipulación de voz, imagen y video. Por lo tanto, el uso de IA en un delito debe ser considerado como un agravante.

Se tiene también el (Reglamento General de Protección de Datos en Europa 2024/1689 del Parlamento Europeo de Inteligencia Artificial, 2024) siendo que toda la Unión Europea ha adoptado dicho reglamento para determinar y regular el uso de IA. Se encarga de prohibir sistemas de IA de alto riesgo que puedan manipular el reconocimiento facial sin consentimiento al establecer estándares de transparencia, supervisión, auditoría y documentación apropiada. Este nuevo régimen del presente reglamento en consideración aparece concebido como una herramienta

de orden público, tal como lo explica (de Miguel Asensio, 2025), su objetivo es precautelar y garantizar los derechos fundamentales frente a las amenazas que pueden presentarse con la IA.

Además, el delito de suplantación de identidad está estipulado en la ley colombiana en su código penal y como lo indica (González, 2025), se tuvo la iniciativa de modificar el apartado de delitos de suplantación de identidad para agregar el aspecto de la IA. En virtud de la figura de falsedad personal, el artículo 296 del Código Penal determina que el individuo que provoque perjuicio, sustituya o suplante a otra persona o se adueñe de su estado civil, nombre, edad o calidad que tenga consecuencias legales, será penalizado con una multa, siempre que el comportamiento no constituyéndose como un nuevo delito. Si bien, varios países de América Latina han firmado acuerdos sobre el uso ético de IA, el Observatorio de Riesgos Catastróficos Globales (ORCG) detalló que una de las naciones con más avances destacables ha sido Colombia. De acuerdo con ese organismo internacional, el país ha diseñado hojas de ruta para la adopción sostenible de la IA, ha suscrito acuerdos con Estados que hacen parte de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y está tramitando cuatro proyectos de ley referentes a esta tecnología.

Por último, el delito de suplantación de identidad se encuentra tipificado en el artículo 172 del Código Penal de la Nación Argentina / Ley 11.179, establece que la persona que defraude a otra con nombre falso, calidad simulada, o cualquier otro ardid o engaño, puede ser penada con prisión de un mes a seis años. Elementos claves a considerar para aplicarse en nuestro contexto, con una pena privativa similar a nuestro COIP.

4. Características

4.1. El delito de suplantación de identidad en el Ecuador

En el Ecuador, la creciente adopción de tecnologías digitales ha traído consigo tanto beneficios como desafíos. El internet ha llegado a ser un canal para transmitir datos y comunicarse, además de convertirse en una herramienta que permite la interacción entre personas en todas las actividades a lo largo y ancho del país. Además, admite que es esencial contar con personal experto en el tema dentro del sistema judicial, así como fomentar desde el Legislativo la implementación de regulaciones y normas más adecuadas que aborden estos usos maliciosos de la inteligencia artificial y todos los aspectos relacionados. Ecuador ha dado los primeros pasos en relación con las leyes existentes sobre información y especificaciones informáticas, lo cual se considera como un paso importante en término de progreso tecnológico en el país en los últimos años, pero es muy claro que la legislación correspondiente específica para regular la IA aún no existe, puesto que quedan impunes los actos relacionados con la tecnología. En el fondo de esta deficiencia legal debe agregarse que este tipo de violaciones es difícil de detectar o perseguir debido a que los objetivos activos trabajan minuciosamente con medios que pueden borrar todo rastro de penetración o consumación del delito. Esto es mencionado por (del Pino, 2021) en su artículo titulado Delitos Informáticos: Generalidades.

El delito de suplantación de identidad, de conformidad a lo que establece el Código Orgánico Integral Penal (COIP) en su Art. 212, menciona que toda persona que por "cualquier forma" es una expresión poco precisa y que resulta demasiada generalizada, puesto que suplante la identidad de alguien más para alcanzar un beneficio para sí mismo o para un tercero será sancionada de uno a tres años con pena privativa de libertad. El artículo mencionado carece de claridad, ya que no se especifican los instrumentos, recursos o métodos que podrían ser requeridos

o suficientes para llevar a cabo la violación. Además, no se menciona qué tipo de ganancia se adquiere o se tiene la intención de conseguir tras llevar a cabo el delito.

4.2. Modalidades o Métodos de Delitos Informáticos Vinculados a la Suplantación de Identidad

4.2.1. El phishing

Así como lo describe (Ali Bravo, 2025): El *phishing* es una técnica de Ingeniería social muy utilizada por el cibercrimen para obtener los datos personales de sus víctimas. Los ataques suelen llevarse a cabo a través de un correo electrónico que supuestamente proviene de una entidad de confianza, como banco, una red social, organismos gubernamentales o cualquier otro tipo de empresa reconocida y de renombre. Podemos decir que es un tipo de fraude que generalmente trata de sustraer la identidad del perjudicado mediante ventanas emergentes o emails falsos. Se define el delito como la apropiación ilegal de datos personales, información de cuentas bancarias o números de tarjetas de crédito o débito. A esta modalidad también se le ha identificado una ramificación que se conoce como el *Spear Phishing o Phishing segmentado*, el cual consiste en atacar determinados grupos de personas, siendo de alto interés los grupos de atención prioritaria o grupos vulnerables de personas.

Para detectar un ataque de phishing, los algoritmos de *machine learning* entrenarán un modelo de clasificación con algunos atributos o reglas para determinar si el sitio será clasificado como phishing o no. El algoritmo funciona, en términos generales, a través del análisis de las propiedades de una URL o del contenido de un sitio web y la creación de un modelo predictivo que se basa en esas cualidades, tal como se indicó al principio, antes de decidir si el sitio es verdadero o falso. Para el cometimiento de phishing existe la herramienta de código abierto

llamada *Zphisher* que sirve para obtener inicio de sesión, contraseñas, *Face ID*, etc, para hacerse pasar por una persona y así acceder a sus datos personales.

4.2.2. El *SPAM*

De acuerdo con la Agencia de Regulación y Control de las Telecomunicaciones, este trata de enviar una gran cantidad de mensajes en forma de publicidad que el usuario no quiere, por eso se le llama correo no deseado. Estos mensajes pueden ser correos electrónicos o mensajes de texto. La finalidad es que la víctima haga clic en el enlace incluido para acceder a una página web sospechosa que está bajo la supervisión del atacante. El objetivo final es robar información confidencial como datos personales, claves de acceso, cuentas bancarias y otros datos similares.

Dicho de otro modo, es un tipo de comunicación digital no solicitada ni deseada en la que se incluye publicidad engañosa, ya sea de servicios o productos al incluir el phishing y la distribución de malware. A menudo, esos mensajes o anuncios que contienen spam también tienen enlaces dañinos. Si el usuario hace clic en ellos, se accede a páginas web de procedencia sospechosa y escasa confianza. Con solo hacer clic una vez, es posible robar información o introducir virus informáticos para engañar a los usuarios.

Esto se relaciona firmemente con lo indicado por (Belcic, 2020) : *El spam es cualquier comunicación no solicitada enviada en masa. Aunque suele enviarse por correo electrónico, el spam también se distribuye a través de mensajes de texto (SMS), soportes sociales o llamadas telefónicas. Los mensajes de spam suelen venir en forma de correos electrónicos promocionales inofensivos.*

4.2.3. *Hacking*

El *hacking* o hackeo se trata de un conjunto de técnicas predeterminadas para malograr un sistema digital al introducirse dentro de este y vulnerando sus medidas de seguridad establecidas en su formato. El hacker se trata del sujeto que penetra el sistema de ciberseguridad, superando sus barreras mediante técnicas como ingeniería informática, o también puede crear la simulación de un ataque y sabotaje. Con ello obtiene un acceso no autorizado dentro del sistema al explotarlo. De este modo lo describe (González Enriquez, 2020), dentro de su informe explicando paso a paso cómo funciona el *hacking* y menciona una frase clave para entenderlo: *"La informática es la ciencia que se ocupa del tratamiento automático de la información usando equipos electrónicos llamados computadores."*

4.2.4. El *pharming*

El *pharming*, según nos lo menciona (Panda Security, 2022), se trata de una combinación de las palabras *phishing* y *farming*, es una estafa en línea similar al phishing, en la que se manipula el tráfico de un sitio web y se roba información confidencial. En este tipo de ciberataque de ingeniería social, los criminales desvían a los usuarios que tratan de entrar a una página web concreta hacia un sitio falso y distinto. El objetivo de estos sitios falsos es capturar los datos de identificación personal (PII) de la víctima, así como sus credenciales para acceder a su cuenta, incluyendo contraseñas, números de cuenta, números de seguro social y otros. Alternativamente, buscan instalar en el ordenador *malware pharming*. Los ciberdelincuentes tienden a asediar páginas web de la industria financiera, que incluyen bancos, portales de pago por internet o sitios de comercio electrónico, normalmente con el propósito último del hurto de identidad.

4.2.5. Cracking

Esta modalidad supera el hacking puesto que consiste en el proceso digital de violar alterar una protección de programa de software ajeno, cuyo objetivo principal es suprimir las medidas de protección con las que el software cuenta, con fines delictivos y maliciosos. Con el paso del tiempo, han aparecido verdaderas *cracking crews*, es decir, equipos que se retan motivados por la posibilidad de ganar de manera ilegal o por tener la aprobación de un conjunto de *crackers*. Los procedimientos de cracking suelen ser menos complejos que muchas técnicas de *hacking* comunes, lo que representa otra razón por la cual los hackers se alejan de lo que consideran una actividad egoísta. Esto haciendo énfasis en lo dicho por (Zemanek, 2004): "*El cracking se puede describir como el grupo de técnicas empleadas para codificar, analizar y estudiar los principios de un programa sin disponer de su código fuente."*

4.2.6. Los *Chatbots*

Son programas que simulan la interacción humana como si se tratara de personas reales, gracias a conversaciones naturales y fluidas con los usuarios. Así como lo indica (UNIR, 2025):"*un chatbot es un software que emplea la automatización, la inteligencia artificial o ambas cosas para conversar en tiempo real con los usuarios de un determinado sistema de mensajería, igual que lo haría una persona."*

Estos softwares se basan en inteligencia artificial generativa o general. Los primeros se limitan a identificar patrones y ofrecer respuestas automáticas. Los segundos imitan las redes neuronales humanas y tienen la capacidad de aprender a partir de interacciones, lo que permite crear diálogos ilimitados y abiertos, ya sea porque están conectados a Internet o porque disponen de bases de datos extensas con contenido diverso.

Existen ciertos elementos transversales en las respuestas de los *chatbots*. Primero, dado que estos programas están diseñados para sostener diálogos naturales y fluidos, lo que supone sustituir la naturaleza humana, también facilitan el fraude, la extorsión, el robo de datos y las estafas para que los usuarios puedan ser víctimas de ellos. En segundo lugar, sus programadores buscan que las IA emulen las redes neuronales humanas. Siguen y persisten en que estas inteligencias artificiales parecen tener la capacidad de sentir empatía. Esto se debe a que se ajustan a una amplia gama de usuarios que interactúan con ellos, lo cual les permite adaptarse a diferentes contextos.

5. Criterio de autor y cierre de ideas

La IA en sí misma representa tanto una oportunidad como una amenaza para la humanidad. Su uso sin aplicar consciencia crítica puede derivar en degradaciones sociales y deterioros cognitivos, emocionales, psicológicos, entre otros riesgos asociados. La IA generativa ha transformado la manera de crear contenido digital, posibilitando la producción de audios, imágenes, videos y textos hiperrealistas. Esta tecnología, en manos equivocadas, puede ser usada para generar *deep fakes* con propósitos engañosos, desinformación o calumnia. En esta línea, la suplantación de identidad usando inteligencia artificial no solamente tiene un impacto sobre las personas, sino que también puede influir en la toma de decisiones públicas o privadas. Pueden poner en riesgo a instituciones y gobiernos, facilitando fraudes y delitos financieros y la estabilidad social en términos generales.

La tecnología progresa y los derechos de los usuarios quedan expuestos a numerosas prácticas ilegales, relacionadas con la IA, que son implementadas por estafadores, atacantes o delincuentes. Es esencial, e incluso se podría afirmar que es imprescindible, establecer reglas a

nivel nacional y comunitario que protejan eficazmente el bienestar social. Esto es necesario para que las personas no queden desprotegidas y sin saber qué normativas defender para salvaguardar sus derechos frente a los ataques tecnológicos e informáticos, en los cuales se convierten en víctimas.

Capítulo II

1. Problema Jurídico

¿Sanciona suficientemente el artículo 212 del COIP la suplantación de identidad realizada mediante herramientas de Inteligencia Artificial?

El principal problema jurídico respecto de la suplantación de identidad mediante inteligencia artificial radica en determinar si el artículo 212 del Código Orgánico Integral Penal resulta suficiente para abarcar las nuevas modalidades en el uso de la IA. El núcleo central del delito consiste en suplantar la identidad de otra persona, la conducta supone entonces atribuirse frente a terceros o dentro de determinada infracción, una identidad correspondiente a otra persona, con la particularidad tecnológica del medio utilizado. Por un lado, la suplantación de identidad tradicional hace referencia al uso de documentos o comunicaciones, mientras que, las herramientas de IA crean representaciones digitales capaces de imitar la voz e imágenes de la víctima. Si bien el artículo 212 no contempla expresamente estas modalidades tecnológicas, su redacción permite analizar su aplicación a través de la expresión “de cualquier forma”.

El artículo 212 del COIP nos indica lo siguiente: *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 utilización de la expresión "de cualquier forma” permite comprender distintos medios de ejecución del delito,

por lo que la ausencia de una referencia expresa a la inteligencia artificial no significa que estas conductas sean automáticamente ajenas al tipo penal. Sin embargo, la norma no contempla expresamente las modalidades digitales avanzadas impulsadas por sistemas de inteligencia artificial, circunstancia que puede generar dificultades interpretativas frente a conductas como la creación de *deepfakes*, la clonación de voz o la manipulación de imágenes y otros elementos identificativos. Por ello, el problema no radica necesariamente en que estas conductas se encuentren fuera del artículo 212 del COIP, sino en que la norma no identifica de manera expresa los medios tecnológicos que actualmente pueden ser utilizados para ejecutar la suplantación de identidad, lo que hace conveniente una mayor precisión normativa que fortalezca la seguridad jurídica.

De acuerdo con lo que menciona (Zaffaroni et al., 2005)*: El sistema penal opera ejerciendo un poder punitivo represivo en forma de criminalización primaria y secundaria. Criminalización primaria es la formalización penal de la conducta en una ley, o sea que es un acto legislativo de prohibición bajo amenaza de pena; más claramente, una conducta está criminalizada primariamente cuando está descrita en una ley como delito.* Esto quiere decir que el sistema penal al tener el poder punitivo en representación del Estado, debe entonces encargarse de tipificar toda conducta ilícita para darle un castigo correspondiente a los responsables de esta misma al haber una represión de conductas al considerarlas dañinas o una amenaza para la sociedad. Es entonces que este poder no únicamente castiga, sino que a su vez selecciona cuáles acciones se convierten en objeto de sanción penal, al formalizar las conductas como un delito en la ley penal bajo amenaza de pena. En el caso analizado, el artículo 212 del COIP contempla la conducta de suplantación de identidad y establece la correspondiente sanción penal. No obstante, la norma no hace referencia expresa a las herramientas de inteligencia artificial como medios tecnológicos susceptibles de ser

utilizados para su comisión, circunstancia que puede generar dificultades de interpretación y evidencia la conveniencia de una mayor precisión normativa.

Esto se relaciona al delito de violación a la intimidad, que consiste en acceder, grabar, publicar, interceptar, difundir la imagen y datos personales de una persona. Puede ser relacionado a la suplantación de identidad con el uso de IA porque al robar los datos de una persona y difundirlos es violar la privacidad. Así como nos lo menciona (Machado Maliza et al., 2020): *Las variables espacio-tiempo se han trastocado al pulsar un clic a través del computador, la lejanía de convierte en inmediatez y nuestras ideas, pensamientos, vivencias y actividades cotidianas, pueden dar la vuelta en tan solo un segundo gracias a las redes sociales; la posibilidad de reproducir, intercambiar y almacenar información de todo tipo ha generado un escenario adecuado para la vulneración de los derechos al honor, intimidad, privacidad y hacia la propia imagen.*

Revisando el artículo 178 del COIP podemos observar su similitud o relación con la suplantación de identidad por medio del uso de IA, puesto que nos dice lo siguiente: *Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.* Esta disposición contempla diversas formas de acceso, reproducción y difusión de datos personales, voz, audio y vídeo por cualquier medio; sin embargo, tampoco incorpora una

referencia expresa a las herramientas de inteligencia artificial. Aunque la ley no mencione específicamente las tecnologías en cuestión, no significa que no se pueda aplicar cuando se usan. Simplemente nos demuestra que es primordial analizar la relación de las leyes actuales con las nuevas formas de cometimiento de delitos. En ocasiones, cuando usamos información personal, fotos, o audios a través de inteligencia artificial, se pueden ver vulnerados varios bienes jurídicos importantes a la vez, dependiendo de lo que se haga específicamente.

En concordancia con lo que nos menciona también (Coglianese, 2024): *La forma en que los algoritmos de aprendizaje automático funcionan de forma autónoma para encontrar patrones en grandes conjuntos de datos ha generado temores de un mundo que, en última instancia, cederá aspectos críticos del control humano a los dictados de la inteligencia artificial. Estos temores parecen verse exacerbados por la opacidad intrínseca que rodea cómo los algoritmos de aprendizaje automático obtienen sus resultados.* Esto quiere decir que la IA ha avanzado de una manera tan significativa que actualmente hay la imposibilidad de regular todo su alcance y lo que esto conlleva. Ha logrado niveles de sofisticación inimaginable hasta tal punto de generar imágenes, códigos o textos con un alto nivel de realismo. Entonces, hay una gran dificultad para diferenciar entre algo real y lo que no es, y localizar al responsable de este tipo de delito de suplantar la identidad de una persona por medio de la generación de clones digitales.

El artículo 212 del COIP no menciona directamente el término *"inteligencia artificial",* y esa falta de especificación podría dificultar el entendimiento de aplicación de esta ley a las nuevas formas de suplantación de identidad. Pero es importante tener en cuenta que esta situación no significa que las acciones realizadas con IA queden fuera de la ley. La frase *"de cualquier forma"* que menciona el artículo es abierta y nos permite incluir diferentes modos de cometimiento de delitos, siempre y cuando los requisitos encuadren en la norma.

En consecuencia, la necesidad de reforma no parte de la inexistencia de una sanción penal, sino de la conveniencia de precisar que los medios tecnológicos, incluidos los sistemas de inteligencia artificial, pueden constituir medios de comisión del delito, fortaleciendo así la seguridad jurídica y la aplicación uniforme de la norma.

2. Argumentos

El ejercicio del Derecho Penal se encuentra limitado por la Constitución y las garantías que protegen los derechos fundamentales. Así como lo determina (Sáenz, 2020): *El Derecho Penal es la facultad sancionadora del Estado que permite la convivencia pacífica entre los miembros que conforman la sociedad panameña; constituyéndose así, en un medio de control social de carácter formal que está supeditado a la Constitución y, por ende, su aplicación debe fundamentarse en el respeto a los derechos humanos y convertirse en su principal garante.* Entendiendo esto podemos concordar que el derecho penal es un instrumento que se utiliza para regular el comportamiento de las personas, en el seno de la sociedad. En otras palabras, el Estado, a través el derecho penal, es el único responsable de la potestad punitiva, es decir, es el único que puede imponer sanciones.

En este contexto, el principio de legalidad es como un escudo que protege a los ciudadanos, Este escudo asegura que el Estado no puede sancionar a nadie sin una justificación válida, clara y definida en la ley como delito. Aunque en la actualidad suene muy usual esta tecnología, no significa que no se pueda aplicar el artículo 212 del COIP, ya que, la ley expresa *"de cualquier forma",* lo que significa que engloba diferentes maneras de realizar un acto. Sin embargo, se logra identificar un pequeño problema, y es que, la ley no hace menciona directamente a las herramientas tecnológicas, como los "*deepfakes"* o la clonación de voz. Esta situación puede hacer que sea ligeramente confuso entender la manera correcta de aplicar la ley en estos casos.

Entonces, la verdadera interrogante legal no debe ser si debemos sancionar a alguien solo por usar inteligencia artificial. Más bien, debe ser, cuándo el uso de inteligencia artificial puede convertirse en una herramienta para cometer un delito que cumple con los requisitos expresados en la ley. En nuestro país, el Código Penal, en su artículo 22 dice que son penalmente relevantes las acciones u omisiones que ponen en peligro o producen resultados lesivos, descriptibles y demostrables. Por lo general, este tipo de acciones afecta lo que llamamos bienes jurídicos protegidos, que justamente son los derechos de los ciudadanos. Por lo tanto, usar una herramienta tecnológica no nos convierte directamente en infractores de la ley. Lo primordial, el analizar lo que el individuo realizó realmente e identificar si encuadra con lo que la ley identifica como un delito.

Además, si bien el COIP en su artículo 13 señala sus propias reglas de interpretación. En el inciso segundo se establece que los tipos penales y las penas se deben interpretar en forma estricta, es decir, respetando su sentido literal de la ley. Sin embargo, es trascendental emplear la teoría de la interpretación teleológica. Con ello entendemos que la finalidad del Código Orgánico Integral Penal es resguardar y proteger los bienes jurídicos de los ciudadanos. Pues se sobreentiende que cada tipo penal que yace en él, se orienta a proteger un derecho en particular. Desde el punto de vista de (Franganillo, 2023), en su artículo La inteligencia Artificial Generativa y su Impacto en la Creación de Contenidos Mediáticos, se menciona: *Que se pone de relieve que la inteligencia artificial (IA) generativa es un área en acelerado progreso que posibilita la creación automatizada de material textual, gráfico, sonoro y audiovisual de elevada calidad. Se estudian los modelos lingüísticos extensos para producir textos y las redes antagónicas generativas que han incorporado capacidades de IA dinámica, lo cual hace posible transformar fotos o descripciones textuales sencillas en videos completos directamente en aplicaciones.*

Asimismo, se menciona la tecnología deepfake para falsificar videos y clonar voces humanas. También se discuten las implicaciones para la propiedad intelectual, la veracidad informativa, la identidad personal y la creatividad humana.

Así, determinamos que es necesario precisar la regulación del delito de suplantación de identidad, ya que puede llevarse a cabo por distintos medios digitales, lo cual, de acuerdo con la doctrina y las leyes internacionales, es un delito informático. Entonces toda acción en la que un sistema de computación actúa como un instrumento o herramienta para el cometimiento de un delito, en el que se violan las libertades y los derechos de la ciudadanía es visto como un crimen cibernético. Esto se considera como un sistema de control ejerciendo moralizador de reforma de normas con la implementación de nuevas tipificaciones o sanciones. En consecuencia, la reforma propuesta no pretende crear una nueva conducta penal independiente, sino explicitar que los medios tecnológicos y las herramientas de inteligencia artificial pueden constituir medios de comisión de la suplantación de identidad, siempre que concurran los elementos establecidos en el tipo penal.

Respecto a las fuentes del derecho pertinentes en base a lo anteriormente mencionado, tenemos primeramente leyes extranjeras con las cuales se podrá realizar un análisis comparado siguiendo el ejemplo de dichos países para su implementación. Entre las leyes extranjeras están: Ley 21.459/2022 de Chile; los Artículos 226-8 y 226-8-1 de la Sección 2: Del daño a la imagen de la persona, del Código Penal francés; Ley de Derechos de Autor Digital 2025 de Dinamarca y el Reglamento 2024/1689 de la Unión Europea. Estas leyes extranjeras presentan precedentes sólidos que nos sirven como bases para la incorporación de nueva legislación dentro del COIP siguiendo su ejemplo, ya que introducen principios para la protección de imagen de una persona perjudicada por el uso de la IA, y su sanción correspondiente.

Para complementar esto e implementarlo dentro del COIP siguiendo el orden del derecho penal, tomemos en cuenta lo dicho por (Luzón Peña, 1988): *el Derecho penal protege o defiende a la sociedad y sus miembros frente a los ataques más intolerables a los presupuestos más elementales de la convivencia social, o en una concepción más conservadora- que tutela y refuerza importantes valores ético-sociales con una considerable fuerza moralizante o-configuradora de costumbres, o en una concepción más crítica que supone un instrumento de represión y dominio de determinados grupos o cla*se. Esto lo podemos relacionar a que, al momento de analizar las leyes extranjeras que utilizaremos como base para adaptarlo lo más similar posible a nuestro contexto social, debemos también observar cómo trasciende el derecho penal en el medio ecuatoriano. El derecho penal al actuar como un escudo defiende a la sociedad y las conductas o actos lesivos que dañan a los pilares de la convivencia social y bienes jurídicos, como en este caso específicamente la identidad de una persona, la propiedad de datos personales y la confianza social. Por lo cual, el derecho penal tiene carácter preventivo y represivo ante la presencia de tales conductas.

En este sentido, la reforma que se propone para el artículo 212 del COIP no busca castigar a las personas por el simple uso de inteligencia artificial. Lo que se quiere precisar es que esta tecnología puede ser un medio para cometer el delito de suplantación de identidad cuando se cumplan todos los elementos del mismo. De esta forma, se busca actualizar la ley para que se adapte a las nuevas maneras en que se cometen delitos, sin dejar de lado las garantías que limitan el poder del Estado para castigar.

3. Criterio de autor

En la actualidad, el fraude digital puede estar presente de cualquier modo y cambiando de forma constantemente. Los ciberdelincuentes utilizan herramientas cada vez más modernizadas, como los *deepfakes* y la inteligencia artificial, para encontrar diversas formas de atacar a la sociedad. Lo que pone en alerta a las empresas de los ataques en los que puedan verse involucrados. Por un lado, la ciberseguridad puede ser usada para hacer el mal, pero por el otro, ayuda a innovar las defensas ante los ataques. Por ello, resulta necesaria la formación y la conciencia en torno a la seguridad para protegerse de los ciberataques basados en inteligencia artificial y asegurar un empleo prudente de esta tecnología en el futuro.

Debemos entender que en la actual era digital, la Inteligencia Artificial, si bien es una herramienta muy útil hoy en día, es importante saberla utilizar de manera adecuada y que además, haya una correcta regulación enfocada a todos sus ámbitos con un enfoque de alfabetización digital de acuerdo con los principios jurídicos que se rigen en todas las materias legales para una correcta armonía social sin perjudicar a terceros. Por ello, debe existir una capacitación respecto al discernimiento de los límites de su uso tanto para usuarios promedio como para los profesionales del derecho, sean los abogados, jueces o peritos informáticos especializados, para de dicha forma llevar a cabo un debido proceso que garantice la protección y garantía de derechos humanos que con el uso de la IA conlleve. La regulación debe ser equilibrada e integral en donde se puedan abarcar todos los ámbitos, y por eso es necesario seguir los modelos ya existentes implementados por otras naciones, para que de esa manera replicarlos de la mejor forma posible a nuestra cotidianidad ecuatoriana, clasificando las herramientas de IA según su riesgo exigiendo transparencia.

4. Conclusiones

La suplantación de identidad por inteligencia artificial es un fenómeno jurídico actual que puede incidir sobre el derecho a la identidad, la seguridad jurídica y otros derechos fundamentales. En Ecuador, el artículo 212 del Código Orgánico Integral Penal castiga a quien suplante la identidad de otra persona para obtener un beneficio propio o para terceros, en perjuicio de una persona.

La expresión “de cualquier forma” deja abierto el modo de ejecución del delito, que puede cometerse mediante distintos medios, incluso con la utilización de determinados instrumentos tecnológicos. Que un delito no exprese explícitamente a la IA no significa que no encuadre en la ley. Al contrario, la inteligencia artificial puede ser una herramienta clave para cometer crímenes, como: modificar imágenes, videos, audios, firmas o documentos, haciéndolos pasar por los de otra persona, como ocurre con los *deepfakes.*

Para que el articulo 212 pueda ser aplicado en estos casos, es primordial, que se respeten los principios básicos de, legalidad y tipicidad. El uso de la IA no genera responsabilidad penal por sí solo. La responsabilidad penal corresponde a la persona que emplea la tecnología para llevar a cabo una conducta que reúne los elementos del delito. En este sentido, el elemento subjetivo corresponde al dolo directo, mientras que el elemento material se configura mediante la atribución de la identidad de otra persona, según la clasificación realizada por (Amores Medina et al., 2025): sus datos, imágenes, voz, documentos u otros elementos identificativos.

La Ley Orgánica de Protección de Datos Personales, por su parte, complementa la protección de los elementos que se usan para construir una identidad digital, sobre todo cuando se trata de datos biométricos, imágenes de rostros, grabaciones de voz u otros datos sensibles, aunque

su aplicación no es en sí misma constitutiva de responsabilidad penal. En virtud de esto, el tratamiento de dichos datos exige un nivel de protección de estos datos exige un nivel reforzado de diligencia. Esta ley funciona como un marco preventivo y regulatorio, al ser la encargada de establecer derechos, principios, obligaciones y consecuencias administrativas originarias de un tratamiento irregular de datos personales, más no posee un valor sancionatorio o punitivo.

Por ello, frente al problema jurídico planteado, consideramos que la norma resulta aplicable, pero requiere mayor precisión. Por tanto, se debería reformar el artículo 212 del COIP para reconocer expresamente a la inteligencia artificial como posible medio de comisión, respetando los elementos esenciales del delito y las garantías propias del Derecho Penal.

5. Recomendaciones

Tras un exhaustivo análisis, se concreta que la modificación pertinente del artículo mencionado quedaría entonces de la siguiente manera:

Art. 212.- Suplantación de identidad con el uso de Inteligencia Artificial. - La persona que, de cualquier forma, incluso mediante el uso de sistemas de inteligencia artificial u otras tecnologías digitales, suplante la identidad de otra persona para obtener un beneficio para sí o para un tercero, será sancionada con pena privativa de 5 a 7 años.

Si las víctimas se encuentran en alguno de los siguientes casos, la pena privativa de libertad será de diez a trece años:

1. Si son niños, niñas o adolescentes o personas en estado de vulnerabilidad.
2. La persona que posea alguna discapacidad o que no tenga la capacidad para comprender la magnitud de la manipulación de su identidad.
3. Cuando se trate de figuras políticas o funcionarios públicos, cuya mala imagen pueda confundir a los ciudadanos.

Para cerrar el problema persistente en el ordenamiento jurídico ecuatoriano, se concluye que es necesario e imperativo seguir el modelo que han creado otros países al implementar articulados relacionados a las conductas ilícitas en las cuales se haga uso de la IA, es decir, se deberá implementar una legislación comparada. Ello se analizará bajo el manto del método del sociólogo y economista Max Weber, quien según (Amzat & Kolo, 2022): "*sostenía que el comportamiento humano se ve influenciado no solo por el libre albedrío individual, sino también por los contextos culturales y sociales, lo que da lugar a patrones reconocibles que él denominó acciones sociales."* Esto al aplicarse al ámbito jurídico permite analizar las leyes de otras naciones, jurisprudencia y tratados internacionales en los cuales el Ecuador ha firmado, para con ese análisis, saber interpretarlo y aplicar lo más prudentemente posible replicando lo logrado por otros países y adaptarlo a nuestro contexto social, promoviendo un equilibrio entre la seguridad e innovación.

Con el fin de llevar a cabo una solución al problema jurídico de manera práctica, proponemos a futuro que se lleve investigación detallada acerca de aquellos elementos esenciales que deben tenerse en cuenta para la tipificación específica del delito informático de suplantación de identidad por medio de Inteligencia Artificial: dolo, daño patrimonial o moral, robo de imagen y de datos personales, medios específicos de cometimiento del delito, consecuencias, agravantes y el nexo causal con herramientas de IA. Estos análisis e indagación requerirían examinar y evaluar el impacto social, como la erosión de la confianza pública al existir el aumento de desinformación sobre los nuevos avances tecnológicos, los desafíos y retos legales que estas tecnologías de vanguardia presentan para las sociedades contemporáneas.

Desde una perspectiva dogmática penal, la tipificación requiere delimitar el tipo penal de manera objetiva para que no quepa la interpretación, sino únicamente una aplicación. El dolo se debe probar no solo en la creación de contenido falso utilizando la IA, sino también en su difusión

malintencionada con un fin lucrativo ilegítimo, esto adecuándose a lo mencionado en el artículo 22 del Código Orgánico Integral Penal. Para ejemplificar ello, una deepfake que pueda simular la voz de una persona se encuadra en la suplantación de identidad agravada, más, la IA complica la atribución de autoría de este delito porque los algoritmos de modelos operativos se caracterizan por funcionar de manera autónoma.

Por ende, uno de los principales desafíos legales al respecto es la obsolescencia probatoria, debido a que actualmente en el Ecuador los peritajes forenses, si bien pueden realizarse en base a un análisis informático, la cadena de custodia digital se diluye al analizar la IA, ya que ciertas herramientas especializadas para dicho análisis forense informático no son aún capaces de detectar programas como, por ejemplo, *Midjounery*, lo que vuelve esto algo inmune a diferenciarse si es una prueba real o no, dado que los operadores de la IA operan en una nube global.

A partir de ello, se recomienda entonces la creación de leyes más firmes y estrictas en el marco del Derecho Penal para impedir que la inteligencia artificial pueda ser utilizada de manera excesiva y peligrosa que deriven en la perpetración de otros crímenes, como fraudes, estafas, difamaciones y extorsiones. entre otras cosas. De esta manera, la respuesta jurídica podrá adaptarse a los avances tecnológicos sin limitar la innovación legítima, garantizando al mismo tiempo una protección efectiva del derecho a la identidad y de los demás bienes que puedan afectarse.

Referencias

Ali Bravo, C. (2025). Qué es el phishing: Guía Completa 2025. *ESET Latinoamérica*, 19.

Amores Medina, G. E., Larrea Del Pozo, R. J., & Alvarado Alija, L. A. (2025). La suplantación de identidad mediante la inteligencia artificial y su adecuación en el COIP. *Universidad Bolivariana del Ecuador*, *8*(31), 2647-2667. https://doi.org/https://doi.org/10.33996/revistalex.v9i31.434

Amzat, J., & Kolo, V. (2022, febrero 22). Max Weber y el surgimiento de la sociología interpretativa. [Blog]. *Research gate*. https://doi.org/https://doi.org/10.2307/jj.8692978.21
Belcic, I. (2020). Qué es el spam: Guía esencial para detectar y prevenir el spam. *Avast Academy*, 20.

Bonilla Yoza, M. M., Geomayra Stefany, C. P., Samantha Michelle, Z. Z., & Mario Javier, M. M. (2022). Uso de la inteligencia artificial en los dispositivos móviles. *Universidad Estatal del Sur de Manabí*, *6*(3), 87-97. https://doi.org/https://doi.org/10.47230/unesum-ciencias.v6.n3.2022.460

Código Orgánico Integral Penal (COIP). (2014). Registro Oficial Suplemento No. 180. https://www.defensoria.gob.ec/codigo-organico-integral-penal-coip/

Coglianese, C. (2024, enero 15). Cómo regular la inteligencia artificial [Blog]. *The Regular View*. https://www.theregreview.org/2024/01/15/coglianese-how-to-regulate-artificial-intelligence/

De Miguel Asensio, P. A. (2025). *Reglamento (UE) 2024/1689 de Inteligencia Artificial y Derecho Internacional Privado* (77, p. 14). Revista Española de Derecho Internacional. https://doi.org/https://doi.org/10.36151/REDI.77.1.10

Del Pino, S. A. (2021). Delitos Informáticos: Generalidades. *Universidad Nacional de Ingeniería*, 67.

Franganillo, J. (2023, septiembre 11). *La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos* [Blog]. https://doi.org/http://dx.doi.org/10.17502/mrcs.v11i2.710

García Merino, J. (2024). Suplantación de identidad humana por la inteligencia artificial (IA): Pt. 2. Introducción. *Universidad de la Rioja*, *13*(2), 1-7. https://doi.org/https://orcid.org/0009-0000-3222-6774

González Enriquez, J. (2020). *Hacking Prohibido* (Vol. 1). Ra-Ma. vampy-security.simdif.com/

González, L. M. (2025, octubre 23). Suplantar identidad con IA ya es delito en Colombia: Así se sancionará. *Universidad Central de Colombia*, 10.

Ley que modifica el Código Penal, Decreto Legislativo 635, y la ley 30096, Ley de delitos informáticos, para incluir el uso de la Inteligencia Artificial en la comisión de delitos, 32314, Código penal peruano, Código Penal de Perú Artículos 46 (2025). https://busquedas.elperuano.pe/dispositivo/NL/2394851-2

Luzón Peña, D. M. (1988). *Derecho Penal: Conceptos y Alcance* (Vol. 42). Universidad de Alcalá. https://es.scribd.com/document/379376805/Luzon-Pen-a-Alcanze-y-funcion-del-derecho-penal-1989-fasc-I

Machado Maliza, M. E., Mainato Angamarca, K. S., & Núñez Vaca, A. F. (2020). La violación del derecho a la intimidad por medio de las redes sociales. *Universidad Regional Autónoma de los Andes*, *FA2016000064*, *5*(3), 13. https://doi.org/http://dx.doi.org/10.35381/racji.v5i3.1126

Maldonado Montenegro, C. D. (2025). Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: Desafíos y perspectivas. *Revista Criminalidad*, *66*(3). https://doi.org/https://doi.org/10.47741/17943108.660

Martínez Galindo, G. (2024). *Suplantación De Identidad Digital: Hacia Una Necesaria Tutela Penal: Pt. 3. El Bien Jurídico Protegido De Nueva Generación: La Identidad Digital Como Extensión Del Derecho A La Intimidad*. *ISSN 0423-4847*, *72*(1), 31. https://doi.org/https://doi.org/10.18543/ed7212024

Mejía Terán, D. F. (2025). Caso 700 IA, Entre la protección de datos personales y el uso de la inteligencia artificial. *Uru: Revista de Comunicación y Cultura*, *UASB-E*, (11), 101-116. https://doi.org/https://doi.org/10.32719/26312514.2025.11.7

Panda Security. (2022, septiembre 19). ¿Qué es el pharming? Definición y formas de prevenirlo. *¿Qué es el pharming? Definición y formas de prevenirlo*. https://www.pandasecurity.com/es/mediacenter/pharming/

RAE. (2024). Identidad. En *Diccionario de la Real Academia Española* (p. 1). https://dle.rae.es/identidad

Reglamento General de Protección de Datos en Europa 2024/1689 del Parlamento Europeo de Inteligencia Artificial, 2024/1689, 169 EUR-Lex 14 (2024). https://doi.org/http://data.europa.eu/eli/reg/2024/1689/oj

Sáenz, J. (2020). El DERECHO PENAL COMO MECANISMO DE CONTROL SOCIAL [Blog]. *Academia.edu*. https://www.academia.edu/39048448/El_DERECHO_PENAL_COMO_MECANISMO_DE_CO NTROL_SOCIAL

Turing, A. (1950). *Máquinas de inteligencia y cálculo*. *El juego de imitación*, *1*(59), 433-460. https://doi.org/https://doi.org/10.1093/mind/LIX.236.433

UNIR. (2025). *¿Qué es un chatbot y para qué sirve?* *1*(1). https://www.unir.net/revista/ingenieria/chatbot-que-es/

van Veen, C. (Director). (2020, marzo 19). Una sentencia histórica de los Países Bajos sobre los estados de bienestar digitales y los derechos humanos [Broadcast]. En *Open Global Rights*. https://www.openglobalrights.org/landmark-judgment-from-netherlands-on-digital-welfare-states/?lang=spanish

Zaffaroni, E. R., Alagia, A., & Slokar, A. W. (2005). *Manual de derecho penal. Parte general* (Universidad de la Rioja). UNIR La Universidad en Internet. https://dialnet.unirioja.es/servlet/libro?codigo=575752

Zemanek, J. (2004). *Cracking Sin Secretos: Ataque Y Defensa De Software (Incluye Cd-R Om)* (ESBOAL, Vol. 1). Ra-Ma. https://www.casadellibro.com/libro-cracking-sin-secretos-ataque-y-defensa-de-software-incluye-cd-r-om/9788478976287/991910?srsltid=AfmBOopBGuF6OKfUyRBoFGtuYA0sRttdiEq8JVk7dMd q9IbXLafa-MTD

DECLARACIÓN Y AUTORIZACIÓN

Nosotras, **Casquete Correa Wendy Solange** con C.C: # 0941744047 y **Yépez Frugone Doménica Fabiola** C.C: # **0926690900**; autoras del trabajo de titulación: **Suplantación de identidad mediante el uso de IA**, previo a la obtención del título de **ABOGADA** en la Universidad Católica de Santiago de Guayaquil.

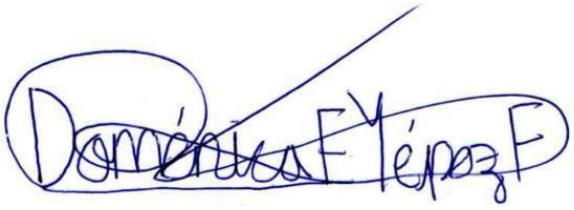
1.- Declaramos tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al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

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

Guayaquil, 25 de agosto del 2026

f. 

Casquete Correa Wendy Solange
C.C: **0941744047**

f. 

Yépez Frugone Doménica Fabiola
C.C: **0926690900**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Suplantación de identidad mediante el uso de IA		
AUTOR(ES)	Casquete Correa Wendy Solange y Yépez Frugone Doménica Fabiola		
REVISOR(ES)/TUTOR(ES)	Abg. Cuadros Añazco, Xavier Paul Mgs.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TITULO OBTENIDO:	Abogada		
FECHA DE PUBLICACIÓN:	25 de agosto de 2026	**No. DE PÁGINAS:**	33
ÁREAS TEMÁTICAS:	Derecho penal, derecho informático, y Protección de datos personales		
PALABRAS CLAVES/ KEYWORDS:	Titular, datos personales, identidad, inteligencia artificial, ciberseguridad, informática		

RESUMEN/ABSTRACT: La Inteligencia Artificial es una herramienta útil en el ámbito laboral, jurídico o académico, pero es un arma de doble filo si no se implementa con regulación y control para evitar su uso malicioso. El eje central de este análisis es la suplantación de identidad por medio de la IA; un problema actual ya que el Código Orgánico Integral Penal (COIP) no regula estos delitos ni el almacenamiento masivo de datos biométricos. Por lo cual, existe una enorme dificultad para identificar responsables en modalidades como deepfakes. Al utilizar medios ilícitos para robar datos personales de un individuo o figura pública, se busca suplantar su identidad creando clones digitales de su voz o imagen, facilitado por la complejidad algorítmica y la falta de sanciones. Ante esta situación, nuestra idea es proponer un conjunto de normas y sanciones claras para quienes incumplen la ley. Por otro lado, queremos sembrar el uso de tecnologías transparentes, y ayudar a que los individuos comprendan de mejor manera el mundo digital actual. Para alcanzar ese objetivo, hemos estudiado leyes de diferentes países de Latinoamérica y la Unión Europea que ya trabajan en el tema en cuestión. Después del análisis profundo de los diferentes acuerdos internacionales que Ecuador ha firmado, creemos conveniente modificar el artículo 212 del COIP, para de esa manera,
evitar confusiones e interpretaciones erróneas.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfonos:** +593958983723 +593985827106	E-mail: domenica.yepez@cu.ucsg.edu.ec wendy.casquete @cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Reynoso Gaute, Maritza Ginette	
	Teléfono: +593-4-3804600	
	E-mail: maritza.reynoso@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA

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