



La suplantación de identidad mediante la inteligencia artificial y su adecuación en el COIP

Impersonation by means of artificial intelligence and its adequacy in the COIP

Falsificação de identidade por meio de inteligência artificial e sua adequação ao COIP

ARTÍCULO ORIGINAL

Galo Emmanuel Amores Medina
geamoresm@ube.edu.ec

Ricardo Javier Larrea Del Pozo
rjlarread@ube.edu.ec

Lissette Amelia Alvarado Alija
laalvaradoa@ube.edu.ec



Universidad Bolivariana del Ecuador. Duran, Ecuador

Escanea en tu dispositivo móvil
o revisa este artículo en:

<https://doi.org/10.33996/revistalex.v9i31.434>

Artículo recibido: 2 de junio 2025 / Arbitrado: 8 de julio 2025 / Publicado: 18 de diciembre 2025

RESUMEN

El artículo aborda la problemática de la suplantación de identidad que se realiza con empleo de inteligencia artificial en Ecuador. El objetivo planteado evaluar la idoneidad del artículo 212 del COIP ante las nuevas modalidades de los nuevos fraudes cibernéticos facilitados por métodos como el deepfake. Se emplea una metodología cualitativa descriptiva y comparativa, analizando estadísticas actualizadas, estudios de caso y criterios doctrinales. Los resultados evidencian un incremento en los delitos cibernéticos y ponen de manifiesto limitaciones en la tipificación del delito en el derecho positivo ecuatoriano que afectan la eficacia de la respuesta penal. Se concluye que es necesaria la reforma del marco jurídico para incorporar criterios jurisprudenciales internacionales, nuevos enfoques sobre la evidencia digital y establecer sanciones adecuadas, a fin de asegurar la protección de los bienes jurídicos en un entorno digital en evolución constante.

Palabras clave: Suplantación de identidad; COIP; Deepfake; Inteligencia artificial; Delitos

ABSTRACT

The article addresses the problem of identity theft carried out with the use of artificial intelligence in Ecuador. The objective is to evaluate the adequacy of article 212 of the COIP in the face of the new modalities of cybernetic frauds facilitated by methods such as deepfake. A descriptive and comparative qualitative methodology is used, analyzing updated statistics, case studies and doctrinal criteria. The results show an increase in cybercrime and reveal limitations in the typification of the crime in Ecuadorian positive law that affect the effectiveness of the criminal response. It is concluded that it is necessary to reform the legal framework to incorporate international jurisprudential criteria, new approaches to digital evidence and establish adequate sanctions, in order to ensure the protection of legal assets in a constantly evolving digital environment.

Key words: Impersonation; COIP; Deepfake; Artificial intelligence; Crimes

RESUMO

Este artigo aborda o problema do roubo de identidade usando inteligência artificial no Equador. O objetivo é avaliar a adequação do artigo 212 da COIP diante das novas modalidades de fraude cibernética facilitadas por métodos como o deepfake. Utiliza-se uma metodologia qualitativa descritiva e comparativa, analisando estatísticas atualizadas, estudos de caso e critérios doutrinários. Os resultados mostram um aumento do crime cibernético e revelam limitações na tipificação do crime no direito positivo equatoriano que afetam a eficácia da resposta penal. Conclui-se que é necessária uma reforma do marco legal para incorporar critérios jurisprudenciais internacionais, novos enfoques sobre provas digitais e estabelecer sanções adequadas, a fim de garantir a proteção dos bens jurídicos em um ambiente digital em constante evolução.

Palavras-chave: Falsificação de identidade; COIP; Deepfake; Inteligência artificial; Crimes

INTRODUCCIÓN

Entre las consecuencias no deseadas del desarrollo tecnológico actual, se encuentra el auge de los denominados delitos informáticos. Dentro de las tipicidades más comunes se encuentra la suplantación de identidad, cuya prevención se complejiza cuando en su realización los comisores acuden a la inteligencia artificial (IA). Se estima que en la actualidad alrededor del 43% de los hechos fraudulentos son realizados con IA y de ellos poco menos de un tercio tienen éxito (Muncaster, 2025). A nivel global se ha apreciado un extraordinario incremento de estos hechos entre 2022 y 2023. En países de Latinoamérica entre los que se incluye Ecuador, se registró en 2024 un incremento de 41% (Coba, 2024). Durante la pandemia de COVID 19, la suplantación de identidad representó casi la mitad de los casos de fraude reportados (2170), de los cuales casi la totalidad se consumó (Zambrano et al., 2023). Estas estadísticas demuestran la magnitud del problema, presentando un panorama socio jurídico que demanda absoluta atención.

Si bien esta forma de criminalidad ha sido históricamente perseguida en la norma penal sustantiva, a lo cual se dio continuidad con la inclusión del artículo 212 del Código Orgánico Integral Penal (COIP) de 2014, la formulación genérica del tipo penal parece insuficiente para cubrir las nuevas modalidades basadas en el uso pernicioso de las tecnologías de la información y las comunicaciones (TIC) y en particular, de la inteligencia artificial (Endara, et al., 2024). Su nocivo impacto económico va más allá de los daños al patrimonio individual para generar una falta de confianza en los sistemas digitales y la consiguiente inseguridad jurídica, estimulada, además, por los bajos niveles de detección y sanción (Muncaster, 2025). Esta situación justifica la realización de investigaciones jurídicas como la que se presenta, cuya utilidad se localiza en identificar las carencias normativas y proponer alternativas de solución.

El crecimiento de los ilícitos penales de este tipo, explican también el aumento de los estudios sobre la suplantación de identidad en diversas latitudes, incluyendo Ecuador. La revisión de numerosos materiales disponibles permite identificar cuatro tendencias: la modelación de fraudes digitales con IA (Alviani y Fitri, 2024) (Subramanian, 2024); los mecanismos para la detección de estos hechos (Zahirah Zahra y Wei, 2023), (Deb, 2024); el desarrollo de sistemas de protección y seguridad informática (Torguatoeva y Osmonaliyev, 2024); así como las revisiones y propuestas de adecuación del marco

normativo de cada país para mejorar la respuesta penal (Recalde, Análisis jurídico crítico del robo de identidad por medios electrónicos como delito autónomo en el Código Orgánico Integral Penal, 2025), (Endara et al., 2024). Sobre esta última línea es la que se profundiza en este estudio.

En el caso específico de Ecuador, autores como Endara et al., (2024), Recalde (2025) y García (2024), sugieren la existencia de debilidades en la cobertura penológica de los ilícitos de fraude identitario con empleo de inteligencia artificial. En todos los casos examinan en profundidad el artículo 212 del COIP desde las perspectivas dogmáticas y socio-jurídicas, sosteniendo la necesidad de una revisión de esta figura penal o la adopción de otras medidas en la jurisprudencia o en materia de políticas públicas.

La problemática jurídica que se define para este estudio está asociada a la efectividad de la norma penal vigente en cuanto a la respuesta a los hechos de suplantación de identidad con empleo del IA. En coherencia con ello el objetivo general del trabajo consiste en analizar jurídicamente los presupuestos o lineamientos para adecuar el artículo 212 del COIP ecuatoriano frente a las nuevas modalidades de suplantación de identidad facilitadas por la inteligencia artificial. Para dar cumplimiento a ese propósito, se formularon tres objetivos específicos. El primero de ellos, realizar análisis de casos emblemáticos recientes sobre suplantación de identidad en Ecuador; el segundo fue realizar un estudio comparado de la legislación internacional que aborda esta tipología delictiva y en tercer lugar, elaborar los fundamentos para una reforma normativa que eleve la capacidad de respuesta de los órganos judiciales.

MÉTODO

La investigación se enmarcó en los estudios sociojurídicos, con predominio del enfoque cualitativo y un diseño descriptivo, analítico y comparativo. Desde esta perspectiva, fue posible examinar de manera crítica la normativa ecuatoriana en relación con los estándares internacionales aplicables a la suplantación de identidad mediante inteligencia artificial. El estudio correspondió a una investigación jurídica aplicada, de carácter exploratorio, explicativo y propositivo, orientada a identificar la problemática existente, profundizar en sus elementos explicativos y construir argumentos que permitieran sustentar posibles adecuaciones normativas (Agudelo, 2020).

En el desarrollo de la investigación se emplearon diversos métodos analíticos. En primer lugar, se aplicó el análisis comparado de la legislación penal relativa a la suplantación de identidad, tomando como referencia los sistemas jurídicos de España, Estados Unidos, Colombia, Perú y Bolivia, con el propósito de identificar enfoques regulatorios y tendencias normativas frente al uso de tecnologías basadas en inteligencia artificial. Asimismo, se recurrió al estudio de casos, seleccionándose situaciones relevantes ocurridas en Ecuador entre los años 2023 y 2025, en las que se evidenció el uso de herramientas de inteligencia artificial para la suplantación de identidad. De manera complementaria, se utilizó el análisis de contenido para examinar informes y documentos emitidos por organismos internacionales especializados en delitos informáticos y protección de derechos digitales.

En cuanto a los criterios de selección de las fuentes, se consideró el factor temporal, excluyéndose materiales bibliográficos anteriores al año 2019, con excepción de las normas legales y doctrinas jurídicas de referencia obligatoria. Dentro del dispositivo metodológico propio de la investigación jurídica, se empleó el método hermenéutico para la interpretación de la legislación pertinente, especialmente del Código Orgánico Integral Penal, mediante el uso de técnicas exegéticas y teleológicas. Adicionalmente, se aplicó el análisis empírico para evaluar estadísticas proporcionadas por organismos nacionales e internacionales, cuyos reportes permitieron identificar tendencias en el comportamiento del fenómeno estudiado. De forma complementaria, se recurrió a recursos del método estadístico con fines descriptivos, particularmente para la representación gráfica de la información analizada.

RESULTADOS Y DISCUSIÓN

En este apartado se exponen las valoraciones y análisis derivadas de la aplicación de los métodos. La exposición de las ideas se realiza en torno a cuatro ejes temáticos.

El delito informático y su tutela penal. Aspectos doctrinales

A través de la historia, la ciencia penal ha evolucionado simultáneamente con el progreso científico técnico, lo cual se expresa en la progresiva incorporación al derecho positivo de figuras penales y

procedimientos emanados del desarrollo tecnológico. Ejemplo de ello son las inclusiones de normas penales para prohibir el uso de sustancias radiactivas, los actos lesivos al medioambiente, el empleo delictivo del espectro radioelectrónico, entre otros, habida cuenta de la peligrosidad de tales comportamientos. En el ámbito jurídico, el término de delitos informáticos comienza a utilizarse desde finales de los años '60 y principios de los '70 del pasado siglo, con la expansión de los sistemas computacionales y las primeras experiencias de la manipulación delictuosa de las computadoras y las redes (Alcalá y Meléndez, 2023).

Muy pronto comenzaron los debates sobre la naturaleza jurídica de esos ilícitos y la forma de afrontarlos. En ese sentido emergió una primera postura denominada Teoría restringida, según la cual los sistemas informáticos son meros instrumentos o medios afines para afectar bienes jurídicos protegidos como la información, el patrimonio, el honor o la fe pública. Desde esa perspectiva los cambios legislativos solo deberían precisar el tratamiento penal de los delitos cuyos comisores se auxilien de recursos informáticos (Navarro, 2023). En contraposición a ella emerge una nueva posición denominada Teoría específica, que declara la necesidad de reconocer como un bien jurídico independiente la seguridad informática, entendida como el sistema de medidas para proteger la información que se procesa con medios digitales y la infraestructura tecnológica que se emplea para generar, almacenar, procesar, transmitir datos e informaciones con medios computacionales (Lou y Véliz, 2025).

Un acercamiento a los más recientes postulados doctrinales en esta materia permite reconocer tres pilares.



Figura 1. Fundamentos doctrinales para el tratamiento de los delitos informáticos.

A pesar de los diversos y profusos estudios sobre el tema, cuando se revisa la legislación internacional salta a la vista la variedad de enfoques y perspectivas, incluso desde la misma denominación del fenómeno se alude a delitos informáticos, ciberdelincuencia o delitos cibernéticos. En la Unión Europea, por ejemplo, se utiliza el término de ciberdelito, aunque omite una definición específica (Europol, 2021). Algo similar ocurre en la legislación norteamericana, como lo comenta en su reporte el Centro de Denuncias de Delitos en Internet (IC3, por sus siglas en inglés) (IC3, 2025).

En el caso de América Latina sucede parecido. En los países del área las legislaciones penales han ido incorporando progresivamente diferentes modalidades del delito tanto en leyes independientes como en la norma penal sustantiva. Como señalan Cernomoretz y Nastas (2023), las definiciones penales son sistemáticamente superadas por nuevas tecnologías que redefinen las ideas originales, a lo que se une el carácter transnacional de estos hechos. Sin embargo, más allá de los conceptos y calificaciones penales, la esencia de la regulación penal gira en torno a los bienes jurídicos atacados y sobre esta perspectiva se realizan las clasificaciones de los delitos informáticos.

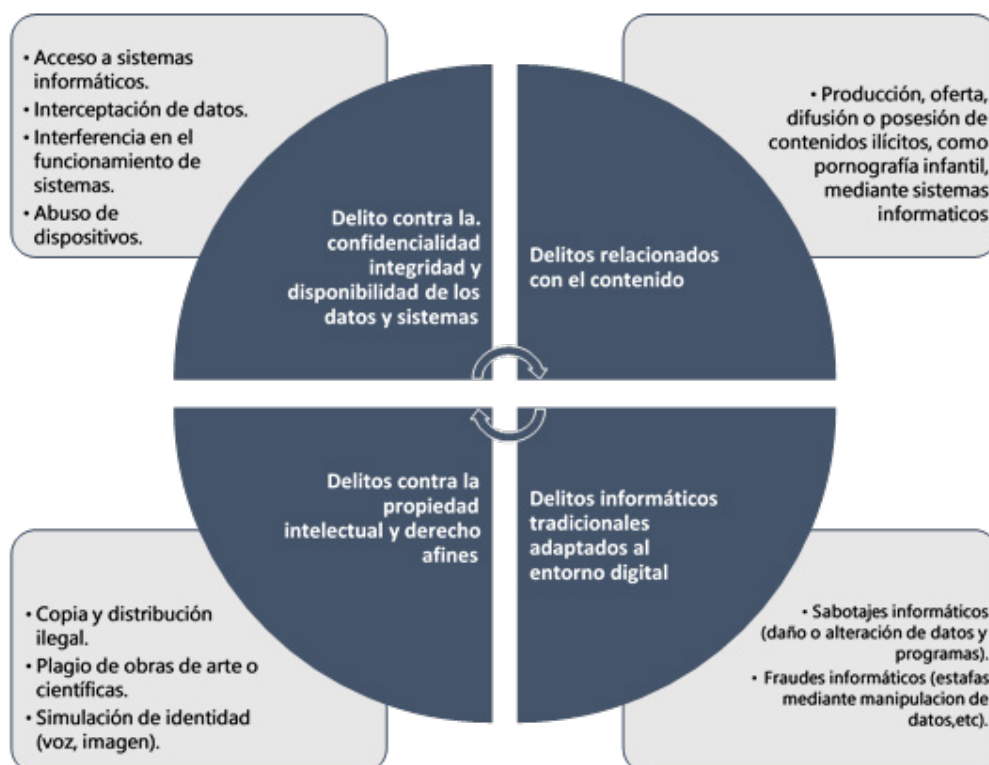


Figura 2. Clasificación de los delitos informáticos.

El primero de estos cuatro grupos de delitos puede realizarse solo con el uso de medios informáticos, es decir, no se trata aquí de que estas tecnologías son un medio afín, sino condición necesaria para la comisión del ilícito. En el resto, se trata de tipologías delictivas más o menos tradicionales, donde el uso de las tecnologías redimensiona la conducta, el peligro, el daño y, en consecuencia, su significación penal. La inteligencia artificial viene a ampliar y “socializar” las posibilidades de uso delictivo de las tecnologías, lo que se aprecia en su empleo como medio para suplantar la identidad de las personas.

El Código Orgánico Integral Penal de Ecuador asume un esquema mixto en la tipificación de los delitos informáticos. Por una parte, define como formas agravadas de los delitos clásicos, el uso de medios informáticos y, desde su puesta en vigor en 2014, introduce la tutela a un bien jurídico que denomina “seguridad de los activos de los sistemas de información y comunicación”, ubicado en la sección tercera del Capítulo Tercero, relacionado con los ilícitos lesivos a los Derechos del Buen Vivir. Dentro de esta familia el legislador ubicó la revelación ilegal de bases de datos (art. 229), la interceptación ilegal de datos (art.230), la transferencia electrónica de activo patrimonial (art. 231), el ataque a la integridad de sistemas informáticos (art.232), los delitos contra la información pública reservada legalmente (art. 233) y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones (art. 234) (COIP, 2014). En su estudio sobre este particular, Saltos et al., concluyen que la ley ecuatoriana “es generalizada en el tema de delitos informáticos, por lo cual, necesita ser reformada y especificada acorde a cada tipo de delito y estar en constante actualización” (2021, p. 350).

La suplantación de identidad desde el derecho comparado. Análisis de la descripción del tipo penal en el COIP

La suplantación de identidad en términos simples, consistente en que una persona se atribuya la identidad de otra. Este comportamiento adquiere relevancia penal cuando la finalidad de esa simulación de identidad está motivada por la búsqueda de beneficio para sí o un tercero, o cuando se persigue causar un daño (animus nocendi). Este delito es una derivación jurídica de la usurpación de estado civil, concebida para proteger la identidad jurídica y social de las personas ante posibles actos fraudulentos (Martínez, 2024). En sus manifestaciones iniciales la suplantación se daba fundamentalmente mediante el uso de documentos apócrifos y otros ardides, pero con el desarrollo tecnológico y la

digitalización, la conducta ha evolucionado, lo que ha generado la necesidad su abordaje penal, tanto desde el punto de vista de la descripción del tipo como de la actividad probatoria.

El elemento subjetivo en el delito de suplantación de identidad es el dolo directo, pues se trata de un acto voluntario, consciente y deliberado, es decir, la calificación no admite la culpa. La acción es cometida por un sujeto genérico, o sea, no se requiere una condición adicional. El elemento material se configura al atribuirse la identidad de otra persona, empleando sus datos personales, documentos, imágenes, firmas, la voz o cualquier otro medio que induzca a terceros a que se identifique al comisor con la persona suplantada.

Las formas de suplantación pueden ser variadas, y van desde el uso de documentos falsificados material o idealmente, la manipulación de datos biométricos, como huellas dactilares o reconocimiento facial, la creación de perfiles falsos en redes sociales o plataformas digitales, hasta la utilización de tecnologías avanzadas como la inteligencia artificial para imitar la voz, la imagen o el comportamiento de la persona suplantada. En cualquier caso, la acción fraudulenta debe ser capaz de inducir a error a terceros, incluyendo entidades (Martínez, 2024).

Es una figura autónoma pues, aunque generalmente se realiza para cometer otras acciones (estafas, robos, defraudaciones, etc.), el solo hecho de atribuirse una identidad falsa con ánimo de lucro o de daño, integra el tipo penal. Se trata, además, de un tipo de delito de peligro, porque la acción suplantadora en sí misma no provoca el daño, pero es necesaria para inducir a otros a cometer errores y actuar de modo conveniente a los propósitos del suplantador (Picón, 2022).

En las legislaciones modernas, es común encontrar formas agravadas de la figura básica, relacionadas con los medios utilizados para la suplantación; los propósitos lucrativos del autor, los ámbitos en que se desarrolla (por ejemplo, la actividad policial, judicial, la salud pública, etc.); los daños eventuales a menores de edad, así como la actuación en composición de grupo criminal organizado. La siguiente tabla ilustra el tratamiento penal de la suplantación de identidad en cinco naciones.

Tabla 1. Comparación del tratamiento del delito de suplantación de identidad.

Países	Denominación del tipo penal	Conductas descritas	Norma reguladora	Sanciones
España	Usurpación de estado civil	Atribuirse el estado civil o identidad de otra persona para obtener beneficios o causar perjuicio.	Código Penal, art. 401	Prisión de 6 meses a 3 años
Estados Unidos	Identity theft (Robo de Identidad)	Uso fraudulento de información personal para cometer fraude, fraude electrónico, postal u otros delitos.	Título 18, sección 1028 del Código Federal	Prisión hasta 15 años y/o multa hasta 250 mil USD
Colombia	Falsedad personal	Suplantar identidad para obtener beneficios ilícitos o causar perjuicio a otro.	Código Penal, art. 296	Multa
Perú	Falsedad genérica	El que comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde.	Código Penal, art. 438	Prisión hasta 3 años
Bolivia	Falsificación de documentos en General	El que falsificare ya sea, material, ideológica, público, privado, uso, supresión, destrucción, etc.	Código Penal, art. 198 al 203	Prisión de 1 meses a 8 años dependiendo

Véase las diferencias de los enfoques adoptados por los legisladores. Donde en algunos casos se alude a la identidad, en otros se menciona el estado civil, lo que introduce una primera divergencia terminológica. Mientras que el estado civil es la condición jurídica de una persona en relación con su situación sentimental o familiar, de la cual se derivan derechos y obligaciones, la identidad es el conjunto de características, que distinguen a una persona o grupo y lo hace único y diferente de los demás. Desde el punto de vista legal, la identidad se avala en documentos que hacen a un individuo titular de derechos y sujeto de obligaciones específicas. De esto se colige que las legislaciones revisadas no tutelan exactamente el mismo bien jurídico, ya que la sistemática seguida busca proteger la fe pública, el derecho a la propia imagen o el estatus jurídico de la persona.

Salta a la vista en los códigos de España, Perú y Bolivia, la usencia de la mención al delito de suplantación de identidad. En estos casos lo que se sanciona es la manipulación o uso doloso de documentos falsos, públicos o privados. Se entiende de esta forma que la suplantación de identidad

se comete cuando alguien usa los documentos identitarios de otro (falsedad ideológica). Al respecto Martínez (2024) la necesidad de una reforma penal del código español.

En línea general, las leyes penales estudiadas sancionan la falsedad o la suplantación per se, o sea, los legisladores, contrario a lo que sucede en el COIP, estimaron que el fingimiento documental es una conducta punible con independencia de sus resultados. También es notable que en los cuerpos legales consultados coexisten diferentes formas de suplantación, ya sea de estado civil, de identidad, de autoridad o funcionario público o de votante. Es decir, predomina un enfoque en virtud del cual la falsedad puede ser una forma de comisión de varios tipos penales.

En el caso de Estados Unidos, se define el robo de identidad, de modo que la calificación penal debería exigir una acción sustractiva previa por parte del autor. La otra diferencia notable reside en el marco sancionador, lo que habla de las diferentes posturas de los legisladores en relación con la peligrosidad del delito.

Ahora bien, ¿cuál es la posición que asume el COIP ecuatoriano en relación con este delito?

Primeramente, debe decirse que la norma penal anterior, el Código Penal de 1938, no recogía expresamente la figura de suplantación de identidad, pues las conductas se incorporaban a otras variedades del fraude como la usurpación del estado civil y la falsificación de documentos. De esta forma habría que reconocer al COIP con la introducción de este delito, a pesar de que algunos autores advierten que la reforma de 2014 implicó cierta descodificación penal (Araujo, 2025). Con la nueva ley sustantiva quedaba recogida en la décima sección del Capítulo Segundo, regulando los delitos contra el derecho a la identidad, el artículo 212, donde se sanciona con uno a tres años de privación de libertad a “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” (COIP, 2014, art. 212).

Al utilizar la fórmula “de cualquier forma”, el legislador abre el espectro de posibilidades en las que se puede realizar la suplantación, lo cual se adecua a los numerosos recursos existentes. Ello, por supuesto, cubre las variantes de suplantación que pueden realizarse mediante sistemas tecnológicos, incluyendo la inteligencia artificial. Sin embargo, cuando se revisa en profundidad la letra de la norma, surgen algunos aspectos susceptibles a debate (Recalde, 2025). Por ejemplo, en la redacción de la primera parte, la frase “para obtener un beneficio”, funciona como complemento circunstancial de finalidad, porque

enuncia el propósito de la acción de suplantar, pero a continuación se yuxtapone otro complemento circunstancial: “en perjuicio de una persona” (Moreno et al., 2022). Esa redacción sugiere que deben cumplirse ambas condiciones, cuando, según la doctrina, el efecto nocivo de la suplantación puede tener uno u otro propósito, de manera que hubiese sido mejor utilizar una disyunción: “...un beneficio para sí o para un tercero o en perjuicio de...”.

En la práctica, una conducta fraudulenta donde la persona suplante la identidad de otra puede ser, exclusivamente obtener un beneficio, considerando como tal la satisfacción de una necesidad personal. Tómese el ejemplo donde un individuo suplanta la identidad de otro para difundir noticias falsas o alarmantes, o para seducir a alguien o sencillamente para obtener elogios. Aquí el beneficio sería satisfacer esa necesidad perniciosa y dañina, más que perjudicar a la persona suplantada. Incluso, puede suceder que el suplantador no quiera en absoluto perjudicar al suplantado: un individuo asume la identidad de un amigo o familiar para actuar en su nombre y obtener algún beneficio, pero adopta medidas para que la suplantación no acarree perjuicios al suplantado (Recalde, 2025). Otro caso sería cuando la suplantación se realiza específicamente para dañar a la persona suplantada mediante mofas, burlas u otras formas de dañar su imagen.

Por otra parte, si bien la suplantación supone, al igual que la usurpación, una acción no consentida o aprobada por la persona suplantada, puede darse el caso en que el propósito de esa falsificación de identidad tenga como finalidad beneficiar a la presunta víctima. Por ejemplo, un familiar usa la identidad de otro para realizar trámites médicos o administrativos, obtener ayudas a favor del suplantado (Flores, 2023). Esta circunstancia plantea una duda sobre si lo que se protege es el derecho a la identidad o la fe pública, es decir, la confianza de las personas o las libertades individuales, o sea, la libertad de elegir una acción. No obstante, queda claro que se trata de un delito pluriofensivo que dificulta su ubicación en la ley penal, como comenta Sánchez Tomás, citado por Martínez (2024).

El otro tema de debate es la falta de elaboración de formas agravadas del delito. Aunque el COIP prevé de manera general las circunstancias agravantes de la responsabilidad penal, son numerosos los tipos penales que incrementan el rigor de la sanción con arreglo a ciertas situaciones. Como se vio anteriormente, la fórmula usada por el legislador subsume todas las modalidades de suplantación, sin embargo, como comentan Endara et al., (2024), el uso de tecnologías como la inteligencia artificial, dada su sofisticación, puede ampliar sustancialmente el daño de la suplantación. De tal suerte, podría ser

conveniente en futuras revisiones, prever sanciones agravadas para este delito cuando se comente por medios que pueden reforzar su efecto defraudador o cuando de él se derivan perjuicios significativos para una persona, entidad o grupo social.

En síntesis, puede decirse que la doctrina internacional es unánime en reconocer la peligrosidad social de la suplantación de la identidad, pero no lo ha sido en la forma de tipificarlo en la norma penal sustantiva. En Ecuador, el COIP innovó en la tipificación de una conducta que antes estaba dispersa, pero la formulación penal adoptada puede ser mejorada en futuros procesos de reforma.

Situación actual en Ecuador. Estudio de casos.

La penetración de las tecnologías en todas las esferas de la vida social no solo ha impactado en la forma en que las personas actúan y se conducen, sino en el propio lenguaje común. En el ámbito del derecho y las ciencias penales, se aprecia una andanada de conceptos técnicos que describen la incontable variedad de fenómenos nocivos que tienen lugar con el empleo de las tecnologías de la información y las comunicaciones. Pero, por supuesto, no se trata de un fenómeno de naturaleza lingüística, sino un entramado de concepciones y postulados que han dado cuerpo a lo que hoy se conoce como derecho informático (ISEC, 2025).

Al analizar los delitos de suplantación de identidad con empleo de los medios informáticos y, en especial con los sistemas de inteligencia artificial, se aprecia un panorama socio jurídico bien complejo. Según un reporte de la Fiscalía General del Estado, la suplantación de identidad era, al menos en el 2023, el tercer delito más frecuente en términos de uso de las tecnologías. Durante el año 2022, 5,879 fueron víctimas de suplantación de identidad en todo el país. Hasta marzo de 2023 se habían acumulado 1,559 denuncias. Específicamente, respecto a los delitos impulsados por el empleo de tecnologías basadas en IA, se ha informado de un incremento significativo del 411% en casos de estafa virtual (Primicias, 2025).

La emergencia de nuevos métodos de suplantación de identidad, denominados genéricamente como deepfake, redimensiona las capacidades de los delincuentes y aumentan la nocividad de su accionar. A ello se suma el hecho de que, a pesar del alto alcance del internet en el país, se estima que alrededor del 8,2% de ecuatorianos es considerado analfabeto digital (Primicias, 2025).

Estudio de casos relevantes de suplantación de identidad con empleo de IA

De acuerdo con lo proyectado, se realizó una búsqueda sobre procesos penales recientes que muestran el empleo de la inteligencia artificial para la suplantación de identidad. Luego de revisar varios reportes de prensa, se seleccionaron cuatro casos donde la comisión del ilícito y el posterior proceso de esclarecimiento, ilustran los objetos atacados, los modus operandi, los daños y la consecuencia ocasionada por la infracción.

Caso 1. Suplantación para extorsión: en diciembre de 2023 se conoció la existencia de una red delictiva que utilizó software de deepfake para replicar digitalmente la voz y la imagen de un ciudadano. Por medio de llamadas telefónicas y el envío de videos manipulados, los delincuentes lograron inducir pánico en la familia de la víctima, exigiéndoles el pago de un rescate a cambio de la liberación del supuesto retenido. La evidencia pericial digital demostró el empleo de algoritmos de inteligencia artificial para recrear de forma fidedigna elementos biométricos y parámetros vocales (Endara et al., 2024). En este episodio se aprecia la complejidad de tipificar conductas híbridas donde coexisten elementos de integración de figuras tradicionales con el uso doloso de las tecnologías.

Caso 2. Suplantación de identidad para fraudes financieros: en julio de 2024 las autoridades de Quito identificaron un perfil en redes sociales con alto realismo, creado con IA, a título de un sujeto con historial crediticio. Los autores, agrupados en red, lograron acceder fraudulentamente a datos bancarios y solicitar créditos a través de plataformas electrónicas, para lo cual se valieron de audios, imágenes y documentos falsos (Primicias, 2025a).

La evidencia pericial en este caso permitió una doble calificación delictiva (fraude y suplantación de identidad) con un impacto significativo en el patrimonio de la víctima. El hecho revela la peligrosidad de esta actividad para la seguridad financiera de la nación, no solo por la pérdida directa de la masa patrimonial de las víctimas, sino por la pérdida de confianza de los ciudadanos en las plataformas oficiales de transacciones financieras. Por otro lado, la elevada sofisticación del delito y su carácter grupal nuevamente ofrece dudas sobre la racionalidad de las penas previstas en el COIP.

Caso 3. Suplantación de identidad en el sector salud: a inicios de febrero de 2024, en la jurisdicción de Quito se identificó una red que, a través de IA, generó videos falsos que simulaban la imagen y voz de reconocidos galenos con el fin de valerse del prestigio de esos profesionales para acceder fraudulentamente a sistemas informáticos de salud. Los autores lograron que se autorizaran procedimientos y tratamientos sin el conocimiento ni consentimiento de los verdaderos profesionales, lo que derivó en reclamaciones fraudulentas de elevados montos económicos. Las pesquisas periciales demostraron el uso de algoritmos cibernéticos para suplantar la identidad de los médicos (Rosero, 2025).

Aquí se aprecia una de las disímiles aristas que avalan la peligrosidad de los delitos de suplantación cometidos con el uso de IA. El caso ilustra la vulneración de uno de los sistemas más sensibles para los ciudadanos: los servicios de salud. Aunque en este caso se perseguía obtener un beneficio financiero, pudiera darse una situación similar en la que autoridades sanitarias suplantadas por delincuentes, indiquen la adopción de medidas sanitarias inadecuadas, tratamientos médicos incorrecto u otra forma de daño.

Caso 4. Suplantación de identidad en perfiles digitales: en la ciudad de Guayaquil, en abril de 2024, una organización delictiva diseñó perfiles en redes sociales para falsificar la identidad de funcionarios del sistema financiero. A través de aplicaciones de mensajería instantánea (Messenger y WhatsApp), entraron en contacto con las víctimas utilizando audios pregrabados y mensajes automáticos que imitaban el estilo comunicacional de funcionarios bancarios. La credibilidad del engaño indujo a las víctimas a autorizar transferencias electrónicas a cuentas controladas por los delincuentes (Primicias, 2025a). Los controles de seguridad fueron sorteados mediante la combinación de datos reales y ficticios.

Como experiencia de este caso, parecido al primero, se revela la necesidad de ajustar, sino el marco jurídico, al menos la capacidad de los sistemas de protección informática de la infraestructura financiera de las entidades privadas y públicas. En el orden procesal, se hace notoria la necesidad de girar la mirada hacia la denominada prueba digital, no solo por lo relevante que resulta en el esclarecimiento de estos delitos, sino también por la posibilidad latente de que ellas sean manipuladas con algoritmos de IA, incluyendo los documentos y declaraciones de testigos.

Caso 5. Suplantación de identidad con contenido sexual mediante inteligencia artificial: en junio de 2025, en una oficina al norte de Quito, la Policía y la Fiscalía General del Estado de Ecuador (FGE) desarticularon una organización delictiva transnacional que operaba simulando un call center. El grupo captaba víctimas a través de falsas ofertas de préstamos, solicitando datos personales mediante enlaces maliciosos. Con esta información, suplantaban identidades y generaban videos falsos de contenido sexual mediante inteligencia artificial, los cuales eran utilizados para extorsionar, y se identificó un equipo dedicado a modificar imágenes y videos para intimidar a las víctimas. Esta modalidad relacionada con el doxing, buscaba vulnerar la honra y privacidad mediante la exposición de datos manipulados. (Televistazo, 2025); (Policia, 2025).

Puede observarse de forma alarmante cómo la inteligencia artificial, aplicada sin control ético ni jurídico, potencia la capacidad de los grupos criminales para ejecutar actos de suplantación de identidad con fines extorsivos. El uso de tecnologías de IA para la generación de contenido falso de carácter sexual, articulado con técnicas de ingeniería social y malware, marca una evolución delictiva que supera los marcos legales tradicionales, se considera que este tipo de casos demandan una urgente adecuación normativa que tipifique de manera expresa la suplantación de identidad mediante IA, incluyendo los efectos sobre la integridad psicológica y la honra de las víctimas, especialmente cuando se vincula a contenidos sexualizados y manipulados digitalmente.

Discusión

De los aspectos sistematizados hasta aquí, se colige que la tutela penal del delito informático ha evolucionado simultáneamente con el desarrollo de la tecnología y el uso pernicioso de los sistemas digitales. Si bien en una primera etapa se apreciaba una tendencia a ajustar la sanción a la peligrosidad derivada del empleo de las tecnologías, la práctica internacional ha arribado al consenso de identificar la seguridad informática como un bien jurídico que reclama protección penal. Sin embargo, la tipificación de esos injustos se ve ante dos importantes desafíos: por una parte, el hecho de que las tecnologías son transversales a todas las esferas de la vida social abre la posibilidad de que figuras delictivas “clásicas” puedan cometerse ahora por medios de herramientas tecnológicas, de modo que el legislador debe decidir entre penalizar de forma especial los ilícitos que se comenten con las TIC o sancionar como

figuras autónomas la utilización dolosa de esos recursos. El otro desafío es mantener la funcionalidad práctica de un sistema penal capaz de asimilar los imprevisibles cambios en las tecnologías. En el caso que ocupa este estudio, por ejemplo, la inteligencia artificial como la conocemos hoy, hace apenas 20 años era vista como una fantasía tecnológica.

El delito de suplantación de identidad es abordado de modos diversos desde el derecho comparado. Al contrastar la legislación de cinco países, se observa que las normas positivas o bien utiliza denominaciones diferentes o varían en los elementos de integración o ubican el delito como componente de bienes jurídicos distintos. En la legislación se emplea una técnica de tipificación de cláusula abierta o *numerus apertus*. Esta variante podría discutirse como una posible limitación de cara al principio de taxatividad como exigencia del principio de legalidad, sin embargo, en pro de la efectividad de la norma para incriminar hechos de esta naturaleza es una ventaja. En cualquier caso, se trataría fundamentalmente de una decisión de política criminal, dada la imposibilidad de abarcar todos los supuestos que se dan y los que con el desarrollo tecnológico se darían en el futuro. No se puede desconocer que el artículo 13 del COIP determina las formas de interpretación de la norma penal (COIP, 2014). En el mismo se invoca el principio de *lex stricta* (inciso b), así como la inadmisibilidad de la analogía en cuanto perjudique al reo o analogía *in malam partem* (inciso c), sobre el cual Quirós (1987) explica abundantemente.

El estudio de casos practicado refleja la aparición de modalidades de la suplantación de identidad que, además de lesionar la fe pública, lesionan otros bienes jurídicos como la seguridad financiera y el patrimonio, el buen nombre y la honra. El empleo de plataformas de inteligencia artificial en estos casos no solo multiplica el efecto defraudador del delito, sino que limitan sustancialmente la posibilidad de su detección y procesamiento de los autores. A ello se une la dinámica impuesta por el empleo creciente de la evidencia digital como parte de los procedimientos probatorios.

El auge de la IA usada con fines delictivos ha impulsado a diversos tribunales internacionales a afrontar, por primera vez, cuestiones relacionadas con la fiabilidad de la evidencia digital generada mediante algoritmos cibernéticos. En el ámbito internacional, se conocen pronunciamientos en esta materia, tal como lo expone Minaggia (2023), quien se cuestionan la adecuación de los mecanismos tradicionales de acreditación de pruebas en el derecho penal.

En países de alto desarrollo tecnológico como Estados Unidos y otras naciones europeas, también se han registrado importantes pronunciamientos jurisprudenciales. Como se explica en el portal del Grupo Ático 34 (2025), se vislumbra la aparición de un subsistema de jurisprudencia específicamente destinado a abordar las implicaciones penales del uso delictivo de la IA. Aspectos como la autoría, la imputabilidad directa e indirecta, la transparencia de las decisiones automatizadas, son sometidas a debate al analizar la relativa autonomía de los sistemas de IA y replantear las responsabilidades de las empresas que producen esos sistemas. En este informe se pone de manifiesto la discrepancia entre las posiciones de los órganos jurisdiccionales en asuntos como la propiedad intelectual derivada de productos generados con IA.

En caso concreto de Ecuador, la creciente preocupación por el aumento de los delitos cometidos con empleo de inteligencia artificial pone un punto de análisis en la estrategia de transformación digital y sus implicaciones para el sistema de justicia penal. En su artículo, Rúales (2023), observa que la atracción de algoritmos y sistemas de reconocimiento de voz o de rostro en la actividad delictiva, ha movilizó a los peritos en función de establecer nuevos protocolos para el análisis de la evidencia digital. Según este autor, apoyado también por la investigación de Alonso y Velazco, (2024), la experiencia judicial reciente y las primeras sentencias relacionadas con fraudes con utilización de IA, evidencian la necesidad de una actualización de la norma, donde se prevean figuras agravadas de los ilícitos cometidos con tecnologías sofisticadas.

A su turno Portilla (2023), argumenta los contrastes existentes entre la legislación ecuatoriana y las normas internacionales. A partir de su análisis propone estudiar las reformas legales que permitan articular conceptos, procedimientos, criterios probatorios, doctrinales y técnicos para elevar la eficacia de la respuesta legal a los ilícitos cometidos con IA.

Propuesta

Considerando los elementos analizados hasta aquí, se presenta una propuesta para la modificación del artículo 212 del COIP:

Art. 212.- Suplantación de identidad- *La persona que de cualquier forma suplante la identidad de otra, será sancionada con pena privativa de libertad de tres meses a un año.*

Con el enunciado anterior se penaliza el solo hecho de suplantar la identidad, con lo cual se protege este bien jurídico. De acuerdo con el carácter limitado de la lesión, se reduce el marco sancionador, el cual se ajustaría a la gravedad del ilícito mediante la introducción de figuras derivadas:

1. Si el hecho se comete para obtener un beneficio para sí o para un tercero o en perjuicio de una persona natural o jurídica, será sancionada con pena privativa de uno a tres años.

Al incorporar el apartado 1, se podrá elevar la envergadura del reproche a esta conducta ilícita cuando las motivaciones sean el lucro propio o de otros o cuando el fin del sujeto es perjudicar material o moralmente a otra persona, sea esta un individuo o una entidad pública o privada. En adición se propone agravar el ilícito considerando la peligrosidad de los medios:

2. Si el hecho se comete empleando tecnologías informáticas, sistemas de inteligencia artificial (incluyendo deepfakes, manipulación de audio/voz, texto automatizado u otros medios digitales) u otros medios capaces de ampliar los efectos nocivos de la suplantación, la pena será de tres a cinco años.

Con la adición del apartado 2 se eleva la sanción a los sujetos cuando en su accionar acuden a recursos tecnológicos que, como es el caso de la inteligencia artificial, pueden reforzar el impacto dañino de la suplantación. De este modo el tipo penal seguiría una tradición referida al agravamiento de la conducta cuya peligrosidad se eleva por la naturaleza de los medios del delito.

Aunque esta no es, técnicamente hablando, una investigación jurídico-propositiva. La propuesta anterior puede constituir un recurso de apoyo a los juristas que, dado el momento, deban acometer la actualización de la norma penal sustantiva. Además de los aspectos recogidos en esta idea de modificación, el legislador puede considerar si se tratará de un caso de concurso material, donde el hecho se sancione con independencia de otros cometidos en ocasión de este. También se podrán valorar otras circunstancias agravantes como:

- Actuar el sujeto formando parte de un grupo organizado
- Si el sujeto se dedica a fabricar, diseñar o comercializar sistemas tecnológicos u otros medios especialmente destinados a facilitar la suplantación de identidad.
- Cuando el efecto de la suplantación lesione intereses sociales o traiga como consecuencia la aparición de estado de pánico o zozobra generalizada, o afectación patrimonial a escala.
- Con el fin exclusivo de dañar la honra, dignidad, reputación o buen nombre de la víctima o de un tercero sin ánimo de lucro o perjuicio patrimonial.

En este último supuesto, habría que hacer una diferenciación respecto al delito de Usurpación y simulación de funciones públicas (art. 287), donde el agente use la suplantación para simular un cargo y ejercer derechos que no le corresponden.

3. Si el hecho involucra la creación, modificación, difusión o amenaza de uso de material sexual explícito sintético (incluyendo deepfakes, montajes audiovisuales u otras representaciones generadas total o parcialmente mediante inteligencia artificial o herramientas digitales), sin consentimiento de la persona afectada, se impondrá pena privativa de libertad de cinco a siete años.

Este apartado específico aborda el agravante del contenido sexual fraudulento, dada su gravedad por el daño psicológico, moral y social a las víctimas, así como su potencial uso (como en el Caso 5 analizado). La pena refleja el alto impacto en la intimidad, honor y dignidad de las personas.

CONCLUSIONES

El análisis realizado viene a reafirmar que la evolución tecnológica, en especial la socialización de la inteligencia artificial ha aportado nuevas modalidades en la comisión de delitos de suplantación de identidad. Aunque el artículo 212 del COIP constituyó un primer avance para reforzar la respuesta penal al fraude identitario, los acontecimientos recientes, en especial casos como los expuestos en este trabajo, revelan limitaciones en la tutela penal de los ilícitos cometidos mediante IA. Las estadísticas recientes exponen una tendencia sostenidamente creciente en el uso del deepfake y otras formas de manipulación digital de la información, para obtener beneficios ilegítimos.

Un breve repaso sobre los estudios en materia de jurisprudencia internacional y nacional pone de relieve el imperativo de conciliar puntos de vista sobre las exigencias probatorias, el ajuste del marco sancionador, la interpretación de la evidencia digital, así como otros aspectos de la dogmática que redunden en la unificación de posiciones en los órganos judiciales en la impartición de justicia. A esto se une la urgencia de hacer frente a las organizaciones criminales que centran su actividad en las defraudaciones con empleo de las tecnologías.

Sobre la base de los análisis realizados, se recomienda analizar la propuesta de modificación normativa antes expuesta y someterla a discusión entre especialistas de derechos penal, de las ciencias informáticas y demás operadores del derecho.

Debe decirse, a modo de cierre, que aunque el artículo se inserta en el movimiento que propugna la actualización de la norma penal ecuatoriana, la solución del problema relacionado con el enfrentamiento a la suplantación de identidad y otros delitos que se comenten con empleo pernicioso de sistemas tecnológicos, debe ir acompañada de cambios en la política penal, el reforzamiento de los sistemas de ciberseguridad, la capacitación de los investigadores policiales, así como de nuevos esfuerzos en la educación ciudadana. Solo con un enfoque integrador se podrá avanzar en la preservación de los bienes jurídicos y la seguridad del Estado de Derecho.

CONFLICTO DE INTERESES. Los autores declaramos que no existen conflictos de intereses para la publicación del presente artículo científico.

REFERENCIAS

- Agudelo, O. (2020). Metodología de la investigación y metódica jurídica ¿Binomio imperfecto? En *Phronesis, Metodología y paradigmas de la investigación jurídica. Fase 2* (págs. 157-169). Universidad Católica de Colombia. Obtenido de <https://archivos.juridicas.unam.mx/www/bjv/libros/13/6227/12a.pdf>
- Alcalá, M., y Meléndez, M. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *PAAKAT: Revista de Tecnología y Sociedad*, 13(24). <https://doi.org/10.32870/Pk.a13n24.759>
- Alonso, J., y Velazco, E. (1 de abril de 2024). Delitos por/ con inteligencia artificial: presente y futuro. Obtenido de *Diariolaley*: <https://diariolaley.laleynext.es/dli/2024/04/05/delitos-por-con-inteligencia-artificial-presente-y-futuro>
- Alviani, A., y Fitri, Y. (2024). Regulaciones legales sobre delitos contra el uso indebido de tecnología de IA (inteligencia artificial) en fraudes de phishing de voz a través de teléfonos móviles. *Jurnal Hukum De'Rechtsstaat*, 10(2), 207–216. <https://doi.org/10.30997/jhd.v10i2.15150>
- Araujo, P. (8 de mayo de 2025). El paradójico proceso de descodificación del Código Orgánico Integral Penal en Ecuador. Obtenido de AP Paulina Araujo Abogados: <https://araujoasociados.net/index.php/articulos/126-articulo-el-paradojico-proceso-de-descodificacion-del-coip-en-ecuador>
- Asamblea Nacional. (2014). Código Orgánico Integral Penal. Registro oficial Suplemento 180. https://doi.org/https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- ATICO34. (13 de mayo de 2025). Jurisprudencia sobre inteligencia artificial. Obtenido de ATICO34: <https://protecciondatos-lopd.com/empresas/jurisprudencia-inteligencia-artificial/>
- Cernomoret, S., y Nastas, A. (2023). Comparative Analysis of Cybercrime in the Criminal Law System. Bucarest: ADJURIS. Obtenido de <https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf>
- Coba, G. (24 de marzo de 2024). Fraudes impulsados por la Inteligencia Artificial aumentan en Ecuador y el mundo. Obtenido de Primicias: <https://www.primicias.ec/noticias/entretenimiento/tecnologia/inteligencia-artificial-fraude-estafa-ecuador/>
- Deb, E. (2024). Explorando el vínculo nupcial entre la neuropredicción y la IA en la justicia penal: Una revisión teórica. <https://doi.org/10.20944/preprints202405.0409.v2>
- Endara, R., Esponzoa, J., López, E., & Santander, J. (2024). *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas*. Análisis jurídico del deepfake en relación a la suplantación de identidad, Ecuador, IX(1), 240-250. <https://doi.org/10.35381/racji.v9i1.3530>
- Europol (6 de 12 de 2021). La Evaluación de Amenazas contra la Delincuencia Organizada en Internet (IOCTA). Obtenido de EUROPOL: <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2014>
- Flores, J. (2023). Análisis del delito informático de suplantación de identidad. *Actualidad Penal*(107), 66-86. Obtenido de <https://actualidadpenal.pe/revista/edicion/actualidad-penal-107/el-delito-de-violacion-sexual-mediante-engano>
- García, J. (2024). Suplantación de identidad humana por la inteligencia artificial (IA). *Innovare Revista de ciencia*. <https://doi.org/10.69845/innovare.v13i2.432>
- IC3. (9 de 5 de 2025). Internet Crime Complaint Center. Obtenido de <https://www.ic3.gov/>
- ISEC. (7 de abril de 2025). ¿Qué es el Derecho Informático y por qué es cada vez más relevante? Obtenido de Universidad de Negocios ISEC: <https://uneg.edu.mx/que-es-el-derecho-informatico/>
- Lou, T., y Véliz, V. (2025). Delitos informáticos: un análisis jurídico integral de las amenazas en el entorno digital. Sede Guayaquil, Carrera de Derecho. Universidad Politécnica Salesiana. Obtenido de <https://dspace.ups.edu.ec/bitstream/123456789/30252/1/UPS-GT006266.pdf>
- Martínez, G. (2024). Suplantación de identidad digital: hacia una necesaria tutela penal. *Estudios de Deusto*, 7(1), 199-228. <https://doi.org/10.18543/ed.3105>
- Minaggia, M. (2023). La inteligencia artificial en el derecho penal: la utilización de algoritmos predictivos. *Estudios sobre Jurisprudencia*, 278-298. Obtenido de <https://repositorio.mpd.gov.ar/jspui/bitstream/123456789/4810/3/Minaggia%20%282023%2c%20278-297%29.pdf>
- Moreno, P., Paucar, C., y Cajas, C. (2022). Regulación global para evitar la suplantación de identidad digital. *Universidad y Sociedad*, 14(6), 690-696. Retrieved from <http://scielo.sld.cu/pdf/rus/v14n6/2218-3620-rus-14-06-690.pdf>
- Muncaster, P. (12 de febrero de 2025). Cómo la inteligencia artificial está facilitando los fraude de identificación. Obtenido de welivesecurity: <https://www.welivesecurity.com/es/seguridad-digital/fraude-identificacion-inteligencia-artificial/>
- Navarro, D. (2023). El concepto de delito informático según la nueva legislación chilena. *Política criminal*, 18(36), 666-689. Obtenido de <https://www.scielo.cl/pdf/politcrim/v18n36/0718-3399-politcrim-18-36-666.pdf>

- Picón, E. (24 de marzo de 2022). El delito de suplantación de identidad. Obtenido de LegalToday: <https://www.legaltoday.com/practica-juridica/derecho-penal/penal/el-delito-de-suplantacion-de-identidad-2022-03-24/>
- Policia. (25 de junio de 2025). Policía Nacional identificó un call center que era utilizado como centro de operaciones de extorsión y estafa en Quito. Obtenido de Policia Nacional del Ecuador: <https://noticias.policia.gob.ec/policia-nacional-identifico-un-call-center-que-era-utilizado-como-centro-de-operaciones-de-extorsion-y-estafa-en-quito/>
- Portilla, P. (2023). Regulación de la inteligencia artificial: análisis comparativo de Ecuador y legislaciones internacionales. Facultad de Jurisprudencia, Carrera de Derecho. Universidad Regional Autónoma de los Andes. Obtenido de <https://dspace.uniandes.edu.ec/bitstream/123456789/17216/1/UT-DER-EAC-010-2023.pdf>
- Primicias (15 de mayo de 2025). El 8,2% de ecuatorianos son analfabetos digitales y eso los hace vulnerables", según policía de ciberdelitos. Obtenido de Primicias: <https://www.primicias.ec/noticias/seguridad/ciberdelitos-ecuador-estafas-analfabetos-digitales-vulnerables/>
- Primicias. (15 de Mayo de 2025a). Fraudes impulsados por la Inteligencia Artificial aumentan en Ecuador y el mundo. Obtenido de Primicias: <https://www.primicias.ec/noticias/entretenimiento/tecnologia/inteligencia-artificial-fraude-estafa-ecuador/>
- Quirós, R. (1987). Introducción a la teoría del derecho penal. Editorial de Ciencias Sociales. Obtenido de <https://biblioteca.uazuay.edu.ec/buscar/item/18381>
- Recalde, D. (2025). Análisis crítico jurídico sobre la Suplantación de identidad por medios electrónicos como un tipo penal independiente en el Código Orgánico Integral Penal. Centro Sur, 9(1), 15–28. <https://doi.org/10.37955/cs.v9i1.374>
- Recalde, D. (2025). Análisis jurídico crítico del robo de identidad por medios electrónicos como delito autónomo en el Código Orgánico Integral Penal. Centro Sur, 9(1), 15–28. <https://doi.org/https://doi.org/10.37955/cs.v9i1.374>
- Rosero, D. (2025). La Inteligencia Artificial utilizada como herramienta en el delito de suplantación de identidad: Consideraciones para su tipificación dentro del Derecho Penal en el Ecuador. Universidad Central del Ecuador. Obtenido de <https://www.dspace.uce.edu.ec/entities/publication/4074f3cc-d5db-4cc9-9ac6-89044114c77a>
- Rúales, B. (13 de junio de 2023). Inteligencia artificial en el derecho penal. Obtenido de Derechoecuador.com: <https://derechoecuador.com/inteligencia-artificial-en-el-derecho-penal/>
- Saltos, M., Robalino, J., y Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. Revista Conrado, 17(78), 343-351. Retrieved from <http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf>
- Subramanian (2024). El dilema legal de los deepfakes: responsabilidad de la IA y los desafíos del robo de identidad digital. Revista Internacional de Investigación Multidisciplinaria, 6(6). <https://doi.org/10.36948/ijfmr.2024.v06i06.31802>
- Televistazo, E. (26 de JUNIO de 2025). Call Center dedicado a extorsión transnacional operaba en Quito. Obtenido de Youtube: <https://www.youtube.com/watch?v=rmMMmmJQU4E>
- Torguatova, B., y Osmonaliyev, K. (2024). Sobre la cuestión de la responsabilidad penal por actos cometidos con el uso de inteligencia artificial con fines delictivos. 1(1), 41-47. <https://doi.org/10.46914/2959-4197-2024>
- Zahirah Zahra, T., y Wei, Z. (2023). Excavación de la identidad del sospechoso mediante el análisis de la evidencia de grabaciones de voz falsas en el caso de perfil del hablante. Notion. <https://doi.org/10.12928/notion.v5i2.8038>
- Zambrano, A., Loor, F., Zambrano, W., y Párraga, R. (2023). Delitos informáticos en tiempos de COVID: REVISIÓN literaria Ecuador. ESPAM. Retrieved from <https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf>