Polo del Conocimiento

Pol. Con. (Edición núm. 111) Vol. 10, No 10
Octubre 2025, pp. 264-284
ISSN: 2550 - 682X
DOI: 10.23857/pc.v10i10.10539

La Suplantación de Identidad Digital en el COIP: Análisis Jurídico de las Dificultades de Aplicación y su Impacto en el Derecho a la Tutela Judicial Efectiva de las Víctimas en Ecuador

Digital Identity Theft in the COIP: Legal Analysis of the Difficulties of Enforcement and its Impact on the Right to Effective Judicial Protection of Victims in Ecuador

Roubo de identidade digital no COIP: análise jurídica das dificuldades de execução e o seu impacto no direito à proteção judicial efetiva das vítimas no Equador

Carlos Fredi Jumbo Guaycha [I]
cjumbo6@indoamerica.edu.ec
https://orcid.org/0009-0003-0260-3411

Correspondencia: cjumbo6@indoamerica.edu.ec

Ciencias Sociales y Políticas
Artículo de Investigación

*** Recibido:** 26 de agosto de 2025 ***Aceptado:** 22 de septiembre de 2025 *** Publicado:** 07 de octubre de 2025

I. Facultad de Jurisprudencia y Ciencias Políticas, Universidad Indoamérica, Quito-Ecuador.

Resumen

La suplantación de identidad digital emerge como uno de los desafíos más intrincados y apremiantes para el sistema judicial ecuatoriano en la era digital. Este artículo profundiza en las complejidades y obstáculos que surgen en la aplicación del artículo 212 del Código Orgánico Integral Penal en los casos de suplantación de identidad en el entorno digital. Se emplea para ello una metodología de carácter cualitativo, sustentada en un enfoque doctrinal, un riguroso análisis normativo-jurídico y una revisión exhaustiva de la jurisprudencia relevante. Los hallazgos de esta investigación desvelan que la inadecuación intrínseca de la tipificación penal actual, diseñada bajo paradigmas tradicionales, genera dificultades interpretativas sustanciales cuando se intenta aplicar a la fluida y compleja realidad del ciberespacio. Específicamente, la ambigüedad en la definición de los elementos típicos, y de manera crucial, la exigencia del "beneficio" como requisito constitutivo del delito, conduce a una exclusión problemática de conductas que, si bien son claramente lesivas para las víctimas, no persiguen un ánimo de lucro directo. En consecuencia, se postula la urgencia de una reforma integral del marco legal y judicial ecuatoriano. Esta reforma debe contemplar, en primer lugar, una actualización de la tipificación penal que incorpore de manera explícita y precisa las particularidades y modalidades de la suplantación de identidad en el ciberespacio. En segundo lugar, se propone la implementación de unidades especializadas descentralizadas, dotadas de los recursos técnicos y humanos necesarios para abordar la complejidad de los ciberdelitos.

Palabras Clave: suplantación digital; COIP; tutela judicial efectiva; ciberdelitos; derechos digitales.

Abstract

Digital identity theft is emerging as one of the most intricate and pressing challenges for the Ecuadorian judicial system in the digital age. This article delves into the complexities and obstacles that arise in the application of Article 212 of the Comprehensive Organic Criminal Code in cases of digital identity theft. A qualitative methodology is used, based on a doctrinal approach, a rigorous normative-legal analysis, and an exhaustive review of relevant jurisprudence. The findings of this research reveal that the intrinsic inadequacy of the current criminal classification, designed under traditional paradigms, generates substantial interpretative difficulties when applied to the fluid and complex reality of cyberspace. Specifically, the ambiguity in the definition of the typical

elements, and crucially, the requirement of "benefit" as a constitutive requirement of the crime, leads to a problematic exclusion of conduct that, while clearly harmful to the victims, does not pursue a direct profit motive. Consequently, a comprehensive reform of the Ecuadorian legal and judicial framework is urgently needed. This reform must contemplate, first, an update of the criminal classification that explicitly and precisely incorporates the specificities and modalities of identity theft in cyberspace. Second, the implementation of decentralized specialized units, equipped with the necessary technical and human resources to address the complexity of cybercrimes, is proposed.

Keywords: Digital impersonation; COIP; effective judicial protection; cybercrimes; digital rights.

Resumo

O roubo de identidade digital surge como um dos desafios mais complexos e urgentes para o sistema judicial equatoriano na era digital. Este artigo investiga as complexidades e os obstáculos que surgem na aplicação do artigo 212.º do Código Penal Orgânico Integral em casos de roubo de identidade digital. É utilizada uma metodologia qualitativa, baseada numa abordagem doutrinal, numa análise normativo-legal rigorosa e numa revisão exaustiva da jurisprudência relevante. Os resultados desta pesquisa revelam que a inadequação intrínseca da atual tipificação penal, elaborada sob paradigmas tradicionais, gera dificuldades interpretativas substanciais quando aplicada à realidade fluida e complexa do ciberespaço. Especificamente, a ambiguidade na definição dos elementos típicos e, crucialmente, o requisito do "benefício" como requisito constitutivo do crime, conduz a uma exclusão problemática de condutas que, embora claramente prejudiciais para as vítimas, não visam o lucro direto. Consequentemente, é urgentemente necessária uma reforma abrangente do quadro jurídico e judicial equatoriano. Esta reforma deve contemplar, em primeiro lugar, uma atualização da tipificação criminal que incorpore de forma explícita e precisa as especificidades e modalidades do furto de identidade no ciberespaço. Em segundo lugar, propõe-se a implementação de unidades especializadas descentralizadas, dotadas dos recursos técnicos e humanos necessários para lidar com a complexidade dos cibercrimes.

Palavras-chave: Personificação digital; COIP; proteção judicial eficaz; crimes cibernéticos; direitos digitais.

Introducción

La revolución tecnológica ha transformado radicalmente las dinámicas sociales y jurídicas contemporáneas, generando nuevas modalidades delictivas que desafían los paradigmas tradicionales del derecho penal. Los ciberdelitos han evolucionado desde simples infracciones informáticas hacia complejas estructuras criminales transnacionales que operan en el ciberespacio, entre varios delitos que puede consumar existe la suplantación de identidad. En este entorno de convivencia, los crímenes son una de esas características negativas que se transforman al mismo tiempo que avanza la sociedad. Así, hace cincuenta años era imposible pensar que surgirían delitos informáticos como la suplantación de identidad, lo que hoy trae consigo graves problemas en el actuar legal y social, tanto en Ecuador como a nivel internacional.

La suplantación de identidad digital se ha consolidado como uno de los fenómenos criminales más lesivos en el contexto de la transformación tecnológica contemporánea. Mendoza Enríquez y Enríquez Rodríguez (2024) señalan que "la rápida transformación tecnológica impone la imperiosa necesidad de actualizar el marco legal para preservar los derechos fundamentales en el entorno digital" (p.31)., especialmente cuando la digitalización de la administración pública y el tratamiento masivo de datos personales exponen a los ciudadanos a nuevas formas de vulnerabilidad. En este escenario, la ciberdelincuencia, que comprende diversas actividades delictivas que atacan tecnologías de la información o que utilizan dichas tecnologías como medio para cometer ilícitos (UNODC, 2022), encuentra en la suplantación de identidad una de sus manifestaciones más perjudiciales. Esta problemática adquiere particular relevancia en Ecuador, donde el crecimiento exponencial del uso de plataformas digitales, combinado con marcos normativos que aún requieren actualización, ha intensificado la exposición de los ciudadanos ante estos delitos, evidenciando la urgente necesidad de que el Derecho evolucione de su rol tradicionalmente reactivo hacia un enfoque anticipatorio que mitigue los riesgos emergentes en el ciberespacio.

El Código Orgánico Integral Penal ecuatoriano (COIP, 2014), promulgado en 2014, tipifica la suplantación de identidad en su artículo 212, estableciendo que "la persona que suplante la identidad de otra para obtener un beneficio para sí o para un tercero será sancionada con pena privativa de libertad de uno a tres años". No obstante, la aplicación de este tipo penal a conductas realizadas en el ciberespacio presenta dificultades interpretativas significativas que comprometen la efectividad del sistema de justicia penal. Como señaló Grabosky (2001), las primeras manifestaciones de la criminalidad informática representaban 'old wine in new bottles' (p. 243),

sugiriendo que estos delitos eran esencialmente crímenes tradicionales cometidos a través de nuevos medios tecnológicos.

Este problema va más allá de lo técnico y normativo, ya que las características específicas de la suplantación digital generan obstáculos sistemáticos que vulneran cada una de estas dimensiones. En este contexto de creciente digitalización y simultánea vulnerabilidad, la presente investigación se propone analizar las dificultades específicas que enfrenta la aplicación del delito de suplantación de identidad digital en el marco del Código Orgánico Integral Penal ecuatoriano.

La hipótesis central que guía este estudio sostiene que las características técnicas del ciberespacio, combinadas con la inadecuación del marco normativo vigente y las limitaciones institucionales del sistema de justicia, generan una vulneración sistemática del derecho a la tutela judicial efectiva de las víctimas de suplantación digital. Esta hipótesis se fundamenta en la premisa de que un sistema legal diseñado para una realidad predigital se torna ineficaz ante la complejidad de la criminalidad cibernética, perpetuando la impunidad y desincentivando la confianza ciudadana en las instituciones judiciales. La investigación espera responder a la pregunta de investigación subsidiaria planteada sobre qué elementos típicos específicos requiere el artículo 212 del COIP para tipificar adecuadamente la suplantación de identidad digital en redes sociales y cómo pueden incorporarse estos elementos respetando los principios de legalidad penal y las particularidades técnicas del medio digital.

La investigación se enmarca en un enfoque cualitativo de carácter jurídico-analítico, orientado a comprender la interacción entre el derecho penal ecuatoriano y la suplantación de identidad digital. Se estructuró en cuatro fases: análisis normativo del artículo 212 del COIP y normas conexas sobre tutela judicial efectiva y ciberseguridad; revisión jurisprudencial de fallos emitidos entre 2014 y 2024; estudio doctrinal especializado en ciberdelincuencia y derechos digitales; y análisis comparado de legislaciones extranjeras relevantes. Se emplearon técnicas de análisis documental y análisis de contenido temático, permitiendo identificar problemáticas como ambigüedad normativa, obstáculos probatorios y limitaciones procesales. La investigación no busca generalización estadística, sino una comprensión profunda y contextual del fenómeno jurídico abordado.

Desarrollo

La Suplantación de Identidad Digital

La suplantación de identidad digital no puede entenderse simplemente como una variante tecnológica de un delito tradicional, sino que constituye una manifestación cualitativamente distinta de la ciberdelincuencia, que exige una conceptualización autónoma. La irrupción masiva de internet y las tecnologías de la información y comunicación ha dado lugar a un nuevo entorno: el ciberespacio, el cual posee características únicas que transforman la manera en que se configuran las conductas delictivas. En este contexto, surgen nuevas modalidades delictivas que afectan bienes jurídicos fundamentales adaptados a las dinámicas de la era digital.

Mendoza et al. (2025) ofrece una conceptualización fundamental al describir los ciberdelitos como aquellas conductas ilícitas que se caracterizan por utilizar la tecnología, ya sea como el medio para cometer el delito, como el objetivo de la agresión criminal, o, en muchas ocasiones, como ambos. En el caso de la suplantación de identidad digital, la tecnología es intrínseca tanto al acto de suplantar (el medio, por ejemplo, una red social o un correo electrónico) como al bien jurídico agredido (la identidad digital en el ciberespacio). Específicamente, la suplantación digital implica la apropiación de elementos identificativos de otra persona en el ciberespacio con el propósito de hacerse pasar por ella, generalmente para obtener algún tipo de ventaja o causar un perjuicio. Esta conceptualización encuentra un sólido respaldo en la doctrina penal especializada. Romeo Casabona y Choclán (2006) define los delitos informáticos como aquellos que "tienen por objeto la agresión a bienes o intereses relacionados con los sistemas informáticos". En el caso particular de la suplantación digital, el bien jurídico protegido trasciende la mera integridad o seguridad de los sistemas informáticos para centrarse en un aspecto más profundo y personal: la identidad personal proyectada y construida en el ciberespacio.

La suplantación de identidad en el entorno digital no solo replica formas tradicionales de engaño, sino que adquiere una dimensión cualitativamente distinta debido a las propiedades inherentes del ciberespacio. Como ha señalado Miró (2012), la naturaleza transfronteriza, descentralizada y propicia al anonimato del entorno digital permite que este tipo de delitos se cometan desde cualquier ubicación del mundo, afectando simultáneamente a múltiples víctimas en distintas jurisdicciones, sin las barreras físicas que limitan los delitos convencionales. Esta capacidad de escalamiento inmediato y global configura un nuevo paradigma delictivo, en el que una sola acción puede tener efectos masivos y casi instantáneos. Además, estas características hacen que la

suplantación digital sea especialmente atractiva para estructuras de crimen organizado transnacional, que aprovechan el anonimato y la dispersión geográfica para cometer fraudes, lavado de activos o trata de personas, utilizando identidades suplantadas como herramientas operativas clave.

Otro elemento diferenciador es la complejidad técnica y probatoria que conlleva su investigación. La persecución de estos delitos requiere conocimientos avanzados en informática forense, redes y ciberseguridad. Factores como la volatilidad de la evidencia digital, el uso de herramientas de anonimato (como VPNs o la red Tor), y la necesidad de cooperación internacional con proveedores de servicios digitales, dificultan la recolección de pruebas y la atribución de responsabilidades. A esto se suma la transnacionalidad inherente al delito, ya que los ofensores pueden operar desde un país, afectar a una víctima en otro, y usar servidores en territorios adicionales, lo que complica la determinación de competencia judicial y los mecanismos de asistencia internacional.

Un eje fundamental para abordar jurídicamente este fenómeno es la identificación del bien jurídico protegido. En el contexto digital, la identidad personal adopta una nueva dimensión: la identidad digital, la cual ha emergido como un bien jurídico autónomo que merece protección específica. Como señala Fernández Burgueño (2012), en la era de la información existe un nuevo derecho a la identidad digital que no se limita a los datos físicos o registrales de una persona, sino que abarca también su presencia, reputación e interacción dentro del ciberespacio. El entorno digital permite a las personas desarrollar relaciones sociales, laborales, académicas y comerciales que pueden verse severamente afectadas por actos de suplantación, produciendo daños no solo a su imagen, sino también a su credibilidad, acceso a servicios, relaciones y oportunidades profesionales.

En este sentido, De Miguel Asensio (2022) destaca tres propiedades clave de la identidad digital que refuerzan la necesidad de su protección penal diferenciada: **la persistencia**, ya que la información digital tiende a mantenerse en línea de forma indefinida, incluso tras intentar eliminarla; **la replicabilidad**, pues los datos pueden ser copiados y difundidos casi instantáneamente sin límites; y **la desterritorialización**, dado que la identidad digital no se encuentra sujeta a fronteras geográficas, dificultando la persecución de delitos y la determinación de la jurisdicción aplicable.

Frente a este panorama, reconocer jurídicamente la identidad digital como un bien jurídico autónomo se vuelve indispensable para una respuesta penal efectiva. En Ecuador, la ineficacia del marco normativo actual se explica, en buena parte, por no haber incorporado estas particularidades

del entorno digital. Por tanto, es urgente que el derecho penal evolucione hacia una concepción que comprenda y proteja adecuadamente la identidad en el ciberespacio, no solo para garantizar los derechos fundamentales de las personas, sino también para consolidar un entorno digital seguro y confiable.

1. Análisis Dogmático del Artículo 212 del COIP en el Contexto Digital

El artículo 212 del Código Orgánico Integral Penal de Ecuador tipifica el delito de suplantación de identidad en los siguientes términos: "La persona que, para obtener un beneficio para sí o para un tercero, suplante la identidad de otra, será sancionada...". Aunque esta disposición representa un avance en el reconocimiento de conductas lesivas vinculadas a la identidad, su redacción evidencia limitaciones estructurales que dificultan su aplicación efectiva en el entorno digital. Desde una perspectiva dogmática penal, tanto el tipo objetivo como el tipo subjetivo presentan ambigüedades conceptuales que comprometen la eficacia del tipo penal ante la creciente sofisticación de las modalidades delictivas en el ciberespacio.

Desde el punto de vista del tipo objetivo, el sujeto activo del delito se define de manera amplia como "la persona que", lo cual configura un delito común, susceptible de ser cometido por cualquier individuo. No obstante, en el contexto de los ciberdelitos, como es el caso de la suplantación digital, se evidencia una realidad mucho más compleja, donde la conducta delictiva puede involucrar una cadena de actores con roles diferenciados como programadores que desarrollan bots, intermediarios que comercializan identidades y operadores que ejecutan la suplantación efectiva. Esta fragmentación operativa desafía los principios clásicos de autoría y participación del derecho penal, pues dificulta la individualización de la responsabilidad penal conforme a los esquemas tradicionales de imputación subjetiva. A ello se suma la problemática semántica de la conducta típica "suplantar la identidad de otra", cuya vaguedad impide una interpretación precisa en el ámbito digital, donde la identidad no es unívoca ni estática, sino un constructo multifacético que abarca desde credenciales de acceso y nombres de usuario, hasta imágenes, voces, datos biométricos y reputación digital.

Así, la aplicación del tipo penal es deficiente por no distinguir entre las múltiples formas en que se puede materializar la suplantación en el ciberespacio. Las conductas van desde la creación de perfiles falsos con datos de terceros en redes sociales, el acceso no autorizado a cuentas electrónicas mediante la apropiación de contraseñas, hasta la generación de contenido audiovisual manipulado mediante tecnologías como los deepfakes. Todas estas modalidades comparten el mismo núcleo

lesivo: la apropiación ilegítima de una identidad digital, pero difieren en su grado de afectación, modalidad de ejecución y potencial lesivo. La norma, al no contemplar esta diversidad, traslada al operador de justicia la carga de decidir si tales conductas se subsumen o no en el tipo penal, lo que ha generado disparidades jurisprudenciales y una aplicación errática e insegura de la norma.

Por otro lado, el tipo subjetivo presenta una deficiencia aún más crítica. La exigencia de que el sujeto activo actúe "para obtener un beneficio para sí o para un tercero" limita de manera injustificada el ámbito de protección penal frente a las múltiples finalidades que pueden motivar la suplantación digital. Esta visión restringida contrasta con la realidad criminológica del ciberespacio, en la cual el objetivo del agresor puede no ser económico, sino psicológico, social o político. En la práctica judicial se observan casos de suplantación con fines de acoso, daño reputacional, venganza, hostigamiento o manipulación social, cuya gravedad es innegable, pero que no encajan dentro del concepto de "beneficio" tradicionalmente entendido como ganancia patrimonial. Esta exigencia deja fuera del alcance del derecho penal una vasta gama de conductas lesivas, contrariando el principio de lesividad, que exige proteger bienes jurídicos relevantes más allá del interés económico. Además, esta limitación fomenta la impunidad y la desprotección de víctimas que, aunque afectadas en su honra, privacidad o integridad psicoemocional, no ven satisfecho su derecho a la tutela judicial efectiva por la inadecuada configuración normativa del delito.

La dogmática penal contemporánea ha insistido en que el análisis del tipo penal debe ser funcional a la realidad social y al bien jurídico protegido. En este caso, la identidad digital, entendida como una manifestación de la personalidad en el entorno virtual, es un bien jurídico autónomo cuya protección exige una normativa adecuada. La concepción actual del artículo 212 del COIP evidencia un rezago normativo que no alcanza a cubrir la complejidad y diversidad de las conductas típicas en el entorno digital. La jurisprudencia nacional refleja esta inadecuación, al presentar criterios contradictorios sobre la configuración del delito, el momento consumativo y la exigencia del beneficio. Mientras algunos tribunales han considerado que la sola creación de un perfil falso constituye suplantación consumada, otros han exigido actos adicionales para configurar el tipo penal, como el uso efectivo de la identidad suplantada. Estas discrepancias, lejos de enriquecer el debate judicial, generan inseguridad jurídica, desigualdad de trato y obstaculizan la respuesta penal frente a este fenómeno creciente.

El artículo 212 del COIP, si bien representa un intento legislativo por afrontar la problemática de la suplantación de identidad, evidencia una estructura dogmáticamente débil e inadecuada para el contexto digital. La redacción del tipo objetivo, por su ambigüedad, y la inclusión del elemento subjetivo del beneficio, por su carácter restrictivo, impiden que el tipo penal cumpla eficazmente su función preventiva y punitiva. Es imperativo avanzar hacia una reforma legislativa que redefina con mayor precisión la conducta típica, elimine la exigencia de beneficio como elemento constitutivo y reconozca expresamente la identidad digital como bien jurídico tutelado, garantizando así la adecuación normativa, la coherencia dogmática y la tutela efectiva de los derechos fundamentales en el entorno digital.

La siguiente tabla sintetiza de manera cualitativa la profunda desconexión existente entre la formulación actual del artículo 212 del COIP y las realidades operativas y lesivas de la suplantación de identidad en el entorno digital.

Tabla 1

Desconexión entre la Tipificación del Art. 212 COIP y la Realidad Digital

Elemento Típico	**Interpretación Actual**	**Realidad Digital No Cubierta**	**Impacto en Tutela Judicial**
"Suplantar identidad"	Amplitud interpretativa, criterios judiciales dispares.	Creación perfiles falsos, uso datos parciales, apropiación de credenciales.	Inseguridad jurídica, tratamiento desigual.
"Para obtener beneficio"	Exigencia restrictiva económica.	Daño reputacional, acoso digital, venganza, disrupción social.	Lagunas de impunidad, víctimas desprotegidas.

Fuente: Elaboración Propia

2. El Principio de Legalidad en el Contexto de la Justicia Digital

En el Estado constitucional de derechos, el principio de legalidad constituye uno de los pilares fundamentales del ordenamiento jurídico, estableciendo que toda actuación del poder público debe encontrarse previamente autorizada por la ley. El artículo 226 de la Constitución de la República

del Ecuador consagra este principio al establecer que "las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley". Este principio adquiere nuevas complejidades en el contexto de la transformación digital del sistema judicial.

Marco Jurisprudencial sobre Seguridad Jurídica Digital

La Corte Constitucional del Ecuador ha desarrollado una comprensión robusta del principio de legalidad en su intersección con la seguridad jurídica digital. En la Sentencia No. 964-17-EP/22, la Corte recuerda que la seguridad jurídica demanda "un ordenamiento jurídico previsible, claro, determinado, estable y coherente que le permita al individuo tener una noción razonable de las reglas del juego que le serán aplicadas" (párr. 39). Además, precisó que para que exista vulneración del derecho a la seguridad jurídica las transgresiones normativas deben tener trascendencia constitucional (párr. 41), y que las autoridades jurisdiccionales deben actuar dentro del marco de sus competencias para proteger los derechos, evitando desnaturalizar las garantías (párr. 42).

El Debido Proceso como Principio Constitucional

La Sentencia No. 546-12-EP/20 (8 de julio de 2020) construye el marco para entender el debido proceso como principio y sus reglas de garantía. La Corte señaló que "el derecho al debido proceso es un principio constitucional que está rodeado de una serie de reglas constitucionales de garantía (art. 76 de la Constitución y sus numerales; por ejemplo, la garantía de no ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal; o la garantía de, en caso de conflicto entre dos leyes de la misma materia que contemplen sanciones diferentes para un mismo hecho, se aplique la menos rigurosa, aun cuando su promulgación sea posterior a la infracción)" (párr. 23.1).

Agregó que "si bien el derecho al debido proceso es el principio que fundamenta las mencionadas reglas de garantía, la suma de estas no agota el alcance de aquel derecho. Así, los casos de violación de las señaladas garantías no son los únicos supuestos de vulneración del derecho al debido proceso" (párr. 23.2); y que "la legislación procesal está llamada a configurar el ejercicio del derecho al debido proceso y de sus garantías […] a través de un conjunto de reglas de trámite" (párr. 23.).

Criterios de Relevancia Constitucional

La Corte también precisó que no toda infracción de reglas de trámite tiene relevancia constitucional: se requiere que, además de violarse la ley procesal, se socave el debido proceso como principio (párr. 23.4). Asimismo, reconoció que "para que la vulneración del derecho al debido proceso se produzca no es condición necesaria que se haya violado una regla de trámite de rango legal, pues bien puede haber situaciones de vulneración atípicas" (párr. 23.5).

Test de Argumentación Completa

En la misma 546-12-EP/20, la Corte recogió un test de tres elementos para identificar vulneraciones constitucionales en acciones extraordinarias de protección: (18.1) una tesis o conclusión que identifique el derecho fundamental presuntamente vulnerado; (18.2) la base fáctica, señalando la acción u omisión judicial imputada; y (18.3) una justificación jurídica que muestre por qué esa acción u omisión vulnera directamente el derecho (arts. 62.1 LOGJCC [sic en el texto original]).

Prueba Digital y Motivación Judicial

Sobre prueba tecnológica, la Sentencia No. 2385-17-EP/21 sostuvo que la valoración probatoria corresponde a los jueces de instancia y que, por su naturaleza, no es materia propia de la acción extraordinaria de protección (párrs. 26-27). En esa causa, al examinar una denuncia virtual y su autoría, la Corte advirtió la falta de nexo causal y cuestionó la ausencia de firma electrónica que permitiera atribuirla al accionado (párr. 33).

Respecto del deber de motivar, la Sentencia No. 2698-19-EP/24 reiteró que, tratándose de garantías jurisdiccionales, el estándar de suficiencia es elevado: las resoluciones deben (i) enunciar las normas o principios en que se fundan, (ii) explicar su pertinencia frente a los hechos, y (iii) analizar si hubo o no vulneración de derechos (párr. 29). A su vez, la 2385-17-EP/21 sistematizó dos escenarios típicos de violación de motivación: insuficiencia (falta de enunciación de normas o de explicación de su pertinencia) e inexistencia de motivación (ausencia total de argumentación) (párr. 29).

Garantías Jurisdiccionales y Justicia Digital

La jurisprudencia ha enfatizado la responsabilidad de los jueces constitucionales en el contexto digital. Como estableció la Corte en la Sentencia No. 964-17-EP/22, "corresponde a los jueces constitucionales velar [por] que las garantías jurisdiccionales no se desnaturalicen para que estas cumplan su propósito de proteger derechos, de otra manera, las autoridades judiciales no garantizarían el respeto a la Constitución, violando la seguridad jurídica" (párr. 53).

Sobre las violaciones de motivación en contextos tecnológicos, la Corte precisó en la Sentencia No. 2385-17-EP/21 que estas se producen principalmente en dos escenarios: "La insuficiencia de motivación, cuando se incumplen alguno de los criterios que nacen de la propia Constitución como son la enunciación de las normas y la explicación de la pertinencia de su aplicación al caso concreto; y 2. La inexistencia de motivación, siendo esta una ausencia completa de argumentación de la decisión" (párr. 29).

Reserva Legal en Actuaciones Digitales

En cuanto a la reserva legal en actuaciones judiciales digitales, la Corte determinó en la Sentencia No. 964-17-EP/22 que cuando las autoridades judiciales actúan fuera del marco legal establecido, "se tramitó una apelación por fuera de un marco legal previo, previsible y público", lo que constituye una vulneración del principio de legalidad que "dejó subsistentes las medidas cautelares constitucionales que previamente fueron revocadas" (párr. 52). Este criterio resulta especialmente relevante para las implementaciones tecnológicas que deben encontrar sustento normativo previo y respetar los marcos procedimentales establecidos.

La jurisprudencia constitucional ecuatoriana ha establecido un marco conceptual robusto para abordar los desafíos del principio de legalidad en la era digital. Los criterios desarrollados por la Corte Constitucional, especialmente la distinción entre el debido proceso como "principio constitucional" y las "reglas constitucionales de garantía", junto con el reconocimiento de "situaciones de vulneración atípicas", proporcionan las herramientas necesarias para evaluar cuándo las implementaciones tecnológicas trascienden la irregularidad procesal para convertirse en vulneraciones constitucionales que requieren tutela judicial efectiva.

Este enfoque jurisprudencial permite articular la innovación tecnológica con las garantías fundamentales. La literatura especializada propone que 'la digitalización de la justicia debe seguir principios de optatividad, identidad y revocabilidad para garantizar que no se vulnere el acceso a la justicia de las personas carentes de alfabetización digital' (Morales-Gálvez, 2022, p. 190). Esta consideración es fundamental para preservar el carácter universal del derecho al acceso a la justicia, asegurando que la transformación digital del sistema judicial fortalezca, en lugar de debilitar, los pilares del Estado constitucional de derechos.

Derecho Comparado

España: La reforma del Código Penal español en 2015 representó un avance significativo al incluir tipos penales específicos que contemplan diversas modalidades de suplantación digital,

diferenciando entre la suplantación con fines económicos, la realizada para cometer otros delitos y la que busca causar perjuicio a la víctima sin beneficio para el autor. Crucialmente, esta reforma eliminó la exigencia del "beneficio" como elemento constitutivo en muchos de los casos de suplantación, reconociendo que el daño puede ser de naturaleza no patrimonial. Además, se establecieron agravantes específicas por el uso de tecnologías, lo que permite una mayor flexibilidad y adaptabilidad a las nuevas formas de comisión del delito. Esta diferenciación y precisión normativa ha facilitado la labor judicial y ha reducido las lagunas de impunidad.

Colombia: Un referente importante en América Latina es la Ley 1273 de 2009 de Colombia, que creó un capítulo específico para los delitos informáticos, incluyendo no solo la suplantación de sitios web, sino también el uso no autorizado de datos personales y la violación de datos personales. Esta legislación integral ha sido complementada con la implementación de unidades especializadas y el desarrollo de protocolos de investigación adaptados a la naturaleza digital de los delitos, lo que ha mejorado las tasas de efectividad en la persecución de estas conductas.

Chile: Chile ha avanzado en la especialización de sus órganos de persecución penal. Ha implementado unidades especializadas de investigación de delitos informáticos dentro del Ministerio Público, dotadas de fiscales y personal técnico capacitado específicamente en la materia. Estas unidades cuentan con protocolos estandarizados de investigación, herramientas tecnológicas adecuadas y, lo que es crucial, canales expeditos de cooperación internacional. Los resultados cualitativos de estas unidades muestran una mejora significativa en la capacidad de respuesta del sistema de justicia, lo que subraya la importancia de la especialización.

Argentina: Este país ha actualizado su marco normativo, contemplando también las particularidades del ciberespacio y adoptando un enfoque más flexible para la persecución de los delitos informáticos, aunque con diferentes niveles de desarrollo en la implementación de unidades especializadas.

Estados Unidos: Su experiencia en ciberseguridad destaca por contar con legislación federal específica como la Computer Fraud and Abuse Act, que establece penas severas para delitos informáticos, incluyendo la suplantación de identidad digital. Su sistema se caracteriza por una robusta cooperación entre agencias federales y estatales, lo que permite una respuesta coordinada en la lucha contra el cibercrimen. (Ordóñez Córdova, 2024) destaca que los desafíos futuros para Ecuador incluyen la necesidad de fortalecer las capacidades técnicas institucionales y mejorar la

cooperación internacional, señalando que el país ha participado en acuerdos y foros internacionales sobre ciberseguridad, pero aún requiere mayor desarrollo en estos aspectos.

Unión Europea: A nivel regional, la Directiva 2013/40/UE establece estándares mínimos para la tipificación de delitos informáticos, obligando a los Estados miembros a adoptar medidas legislativas específicas. Esta armonización normativa regional es fundamental, ya que facilita la cooperación transfronteriza en la persecución de estos delitos, un aspecto crucial dada la naturaleza transnacional de la suplantación digital.

De este análisis comparado, se desprenden elementos fundamentales para mejorar la efectividad en la persecución de la suplantación digital en Ecuador: la necesidad de especialización normativa, la capacitación continua, la creación de unidades especializadas con recursos adecuados, el desarrollo de protocolos de investigación adaptados a la evidencia digital y el fortalecimiento de la cooperación internacional.

Tabla 2

Propuestas de fortalecimiento institucional del sistema de justicia penal

Área	Propuesta Específica	Justificación	Modelo Referencial
Institucional	Descentralización Unidad Especializada en 4 regiones.	Mejorar cobertura nacional y tiempos de respuesta.	Colombia
Técnica	Laboratorios forenses digitales regionales.	Descentralizar análisis de evidencia.	España
Normativa	Incluir Art. 212 en competencias especializadas.	Garantizar investigación especializada.	N/A
Internacional	Convenios bilaterales de cooperación digital.	Superar barreras jurisdiccionales.	Convención de Budapest.

Fuente: Elaboración Propia

Discusión

La suplantación de identidad digital constituye un desafío jurídico profundo para el sistema penal ecuatoriano, tanto por su naturaleza técnica como por el desfase entre la realidad digital y el marco normativo vigente. Como se ha evidenciado a lo largo de esta investigación, el artículo 212 del

COIP presenta limitaciones dogmáticas que obstaculizan la persecución eficaz de estas conductas. La exigencia del "beneficio" como elemento constitutivo del tipo penal excluye supuestos lesivos que no persiguen fines económicos, como el acoso, la venganza o el daño reputacional, dejando a las víctimas sin posibilidad de una tutela judicial efectiva.

Este déficit normativo no es solo un problema técnico de redacción legal, sino que genera consecuencias directas en los derechos fundamentales de las personas. Al no reconocer de forma explícita a la identidad digital como un bien jurídico autónomo, el ordenamiento penal ecuatoriano no logra proteger adecuadamente la dimensión digital de la personalidad, lo que implica una regresión en materia de garantías frente a la evolución de las formas de criminalidad contemporánea. La rápida transformación tecnológica impone la imperiosa necesidad de actualizar el marco legal para preservar los derechos fundamentales en el entorno digital. En un escenario donde la digitalización de la administración pública, la automatización de procesos y el tratamiento masivo de datos personales son protagonistas, el Derecho debe dejar de ser meramente reactivo para anticipar y mitigar los riesgos emergentes en el ciberespacio. Como señala Granero (2025), este camino hacia una coexistencia armoniosa entre la innovación y la protección de derechos exige un compromiso efectivo de legisladores y autoridades para reordenar y actualizar las normativas, garantizando así la privacidad, la integridad de la identidad digital y la seguridad en el manejo de la información personal (p. 157).

Además de las deficiencias sustantivas, el sistema judicial enfrenta obstáculos procesales y estructurales que profundizan la vulneración del derecho a la tutela judicial efectiva. Según el (Banco Mundial 2022), "la mayoría de los jueces desconocen a profundidad los delitos informáticos y los temas técnicos, como el reconocimiento de la evidencia digital" (p. 80), y de los tres actores del sector de justicia criminal, "la función judicial tiene capacidades más limitadas en el ámbito de los ciberdelitos" (p. 80). Las víctimas deben atravesar un proceso burocrático marcado por la desinformación, la revictimización y la falta de personal capacitado. La Unidad de Delitos Cibernéticos de la Policía Nacional opera con apenas 21 investigadores para todo el país, manejando un promedio de 200 investigaciones por agente, lo que genera "una carga laboral muy alta" que "impide avanzar más rápido en las investigaciones" (Banco Mundial, 2022, p. 79). Esta situación se agrava considerablemente por la falta de conocimiento especializado: el Consejo de la Judicatura "desde hace tiempo no realiza capacitaciones sobre evidencia digital u otros temas relevantes para resolver casos de delitos informáticos" y "los jueces, en general, no comprenden

los temas técnicos relacionados con los delitos informáticos" (Banco Mundial, 2022, p. 80). La inexistencia de protocolos claros y especializados, sumada a la ausencia histórica de una fiscalía especializada en delitos informáticos hasta junio de 2022, incrementa significativamente el riesgo de impunidad.

En este escenario, la experiencia comparada aporta insumos valiosos. Como señala Martínez Galindo (2024), el Código Penal español no sanciona el mero hecho de suplantar la identidad de alguien, sino los comportamientos que se llevan a cabo a posteriori, lo que evidencia la necesidad de una reforma que reconozca las afectaciones extrapatrimoniales de la suplantación digital, más allá del tradicional requisito de beneficio económico. Colombia, por su parte, ha impulsado reformas normativas e institucionales orientadas a la especialización y la investigación digital, permitiendo una mejor persecución de estos delitos (Ley 1273 de 2009). La tendencia común en estos países es clara: actualizar los tipos penales, reconocer la identidad digital como bien jurídico protegido y crear unidades técnicas especializadas que operen con autonomía y recursos suficientes.

Frente a este panorama, el Ecuador requiere una reforma integral en tres niveles: normativo, procesal e institucional. En lo normativo, resulta imprescindible una modificación del artículo 212 del COIP que elimine la exigencia del beneficio y establezca con claridad las distintas formas de suplantación digital, contemplando agravantes específicas. En el ámbito procesal, deben implementarse protocolos para la conservación urgente de evidencia digital, establecer plazos procesales adecuados a la complejidad de los ciberdelitos y permitir mecanismos de cooperación directa con proveedores internacionales. Finalmente, a nivel institucional, urge la creación de unidades especializadas en ciberdelitos con presencia territorial, así como un laboratorio forense digital que permita la conservación y análisis técnico de pruebas con estándares de cadena de custodia.

En términos de política criminal, no se trata simplemente de castigar más o endurecer penas, sino de garantizar que el sistema judicial responda de forma eficaz y proporcional al fenómeno de la suplantación digital. La inacción de los Estados frente al crecimiento exponencial de la ciberdelincuencia genera un vacío de protección que deja a las víctimas en una situación de indefensión. Como señalan varios autores, el fracaso de las autoridades en investigar y sancionar estos delitos no solo perpetúa la impunidad, sino que también crea una percepción de que el ciberespacio es una zona sin ley. Esto, a su vez, socava la confianza ciudadana en las instituciones

judiciales y en la capacidad del Estado para garantizar la seguridad y los derechos fundamentales en el entorno digital, lo que profundiza la brecha de desigualdad entre las víctimas de delitos tradicionales y las de crímenes cibernéticos (Estrada Salvador Ramirez, 2024).

La investigación desarrollada no sólo confirma la hipótesis planteada, sino que evidencia la urgencia de una transformación profunda que permita al derecho penal ecuatoriano insertarse de forma coherente en la sociedad digital. La adecuación normativa, la especialización técnica y la cooperación internacional deben entenderse no como opciones, sino como obligaciones constitucionales del Estado ecuatoriano para garantizar el derecho de las víctimas a una justicia real, oportuna y efectiva.

Conclusiones

La presente investigación ha demostrado que el marco normativo ecuatoriano vigente, en particular el artículo 212 del Código Orgánico Integral Penal, resulta insuficiente para enfrentar adecuadamente la problemática de la suplantación de identidad digital. La exigencia del "beneficio indebido" como elemento del tipo penal limita gravemente la protección de la identidad digital como bien jurídico autónomo, dejando desprotegidas a las víctimas de afectaciones no patrimoniales como el daño moral, el acoso o la usurpación de personalidad.

Las barreras de acceso a la justicia cognitivas, institucionales y económicas vulneran el derecho a la tutela judicial efectiva, consagrado en el artículo 75 de la Constitución de la República del Ecuador y desarrollado por la jurisprudencia nacional e interamericana. Estas barreras impiden que las víctimas puedan interponer denuncias con eficacia, acceder a una defensa técnica especializada, y obtener una reparación integral oportuna, lo cual configura una forma de denegación de justicia material.

El análisis comparado permitió establecer que países como España y Colombia han avanzado en el reconocimiento de la identidad digital como objeto de protección penal autónoma, eliminado elementos restrictivos del tipo penal, e impulsando la creación de unidades institucionales especializadas con competencias técnicas y territoriales. Estas experiencias constituyen referencias fundamentales para el desarrollo de una política criminal ecuatoriana acorde con la complejidad del entorno digital.

Por tanto, es imprescindible, una reforma integral en tres niveles: (i) reforma normativa, que redefina el delito de suplantación de identidad digital con base en la protección de la identidad

como derecho personalísimo, sin requerir beneficio económico; (ii) reforma procesal, que establezca mecanismos expeditos para la conservación de evidencia digital, plazos adecuados a la naturaleza de los ciberdelitos, y protocolos de cooperación internacional; y (iii) fortalecimiento institucional, mediante la creación de unidades especializadas en ciberdelitos, laboratorios forenses digitales y mecanismos de atención integral a víctimas.

El Estado ecuatoriano debe asumir como una obligación constitucional y convencional la adecuación de su sistema penal al entorno digital. Esto no solo implica sancionar con eficacia a los autores de estos delitos, sino garantizar a las víctimas una respuesta judicial real, oportuna y efectiva que respete su dignidad, restituya sus derechos y restaure su confianza en la justicia.

Referencias

Argentina. Ley 26.388 de 2008, de 4 de junio, de Delitos Informáticos. Boletín Oficial de la República Argentina No. 31.436 de 25 de junio de 2008.

Banco Mundial. (2022). Diagnóstico de las capacidades de ciberseguridad del Ecuador 2022. Ministerio de Telecomunicaciones y de la Sociedad de la Información. https://www.telecomunicaciones.gob.ec

Colombia. Ley 1273 de 2009, de 5 de enero, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial No. 47.223 de 5 de enero de 2009.

Corte Constitucional del Ecuador. (2014). Sentencia N.° 136-14-SEP-CC [Caso N.° 0148-11-EP]. 17 de septiembre de 2014.

Corte Interamericana de Derechos Humanos. (2004). Caso Servellón García et al. vs. El Salvador. Sentencia de 23 de julio de 2004. Serie C No. 107.

De Miguel Asensio, P. (2020). Protección de la identidad digital en el entorno transfronterizo. Revista Española de Derecho Internacional, 72(1), 1–27. https://doi.org/10.5944/redi.72.2020.27015

España. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, núm. 77, de 31 de marzo de 2015, pp. 27061-27176.

Estrada Salvador Ramirez, C. T. (2024). La impunidad en los delitos informáticos. Una problemática de poco interés por los legisladores, jueces y fiscales. Ius vocatio, 91-115. https://doi.org/10.35292/iusVocatio.v7i9.928

Fernández Burgueño, P. (2012). "Aspectos jurídicos de la identidad digital y la reputación online". AdComunica, (3), 125–142

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243-249.

Granero, H. R. (with Altamiranda, M., Bonhote, L. V., Brun, J. M., Bugvila, A., Cherñavsky, N., De Venezia, L., Mass, R., Docimo, R., & Farinella, F.). (2025). Inteligencia Artificial en el Derecho: Entre la Innovación y la Protección de Derechos (1st ed). ELDIAL.COM.

Martínez Galindo, G. (2024). Suplantación de identidad digital: hacia una necesaria tutela penal. Estudios de Deusto, 72(1), 199–228. https://doi.org/10.18543/ed.3105

Mendoza Enríquez, O. A., & Enríquez Rodríguez, L. L. (2024). La rápida transformación tecnológica impone la imperiosa necesidad de actualizar el marco legal para preservar los derechos fundamentales en el entorno digital. En Desafíos del derecho a la protección de datos personales en la era digital: una mirada desde América Latina (p. 31). Tirant lo Blanch.

Mendoza, F. F., Leal, Á. J., Salvadori, I., & Castán, C. T. (2025). Cibercrimen: Tendencias y desafíos actuales. Boletín Oficial del Estado.

Ministerio Público de Chile. (s.f.). Unidad Especializada en Delitos Informáticos.

Miró Llinares, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons Ediciones Jurídicas y Sociales.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2022). Compendio de ciberdelincuencia organizada. Naciones Unidas. https://sherloc.unodc.org.

Ordóñez Córdova, L. A. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. Reincisol, 3(5), 1447-1469.

Romeo Casabona, C. (2006). La protección penal de los datos personales. Boletín Mexicano de Derecho Comparado, 39(117), 385–405.

Unión Europea. Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Diario Oficial de la Unión Europea L 218, 14 de agosto de 2013, pp. 8-14.

United States. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.