https://revistalex.org
Volumen 8, No. 29, abril-junio 2025
ISSN: 2631-2735
Páginas 559 - 572

Los ciber delitos y la protección de datos personales en el sistema penal ecuatoriano

Cybercrime and the protection of personal data in the Ecuadorian criminal justice system

O crime cibernético e a proteção de dados pessoais no sistema de justiça criminal do Equador

ARTÍCULO ORIGINAL

Geovanna Gabriela Espinosa Carvajal
gabrieladerechoindoamerica@gmail.com

Fernando Eduardo Paredes Fuentes
fernandoparedes@indoamerica.edu.ec

Universidad Tecnológica Indoamérica. Ambato, Ecuador

Escanea en tu dispositivo móvil
o revisa este artículo en:
https://doi.org/10.33996/revistalex.v9i28.302

Artículo recibido: 8 de enero 2025 / Arbitrado: 10 de febrero 2025 / Publicado: 1 de abril 2025

RESUMEN

El estudio examina los ciberdelitos y la protección de datos personales en el sistema penal ecuatoriano, destacando posibles limitaciones legales y operativas que dificultan su adecuada sanción, señalando ambigüedades en la tipificación de estos delitos en el Código Orgánico Integral Penal y su débil conexión con la Ley Orgánica de Protección de Datos Personales, entre los delitos más comunes figuran el acceso no autorizado a sistemas informáticos, la suplantación de identidad, el ciberacoso y la estafa, los cuales afectan la privacidad y seguridad digital de los ciudadanos, el presente estudio se realizó mediante métodos cualitativos y críticos, revisión de la legislación y jurisprudencia evidenciando vacíos normativos y una aplicación insuficiente de las leyes, lo que fomenta la impunidad y expone a las víctimas, se concluye que es urgente actualizar el sistema penal, para mejorar los recursos judiciales y sensibilizar a la ciudadanía para proteger sus datos personales e incentivar la denuncia de ciberdelitos.

Palabras clave: Ciberdelitos; Protección de datos; Sistema Penal ecuatoriano

ABSTRACT

The study examines cybercrimes and the protection of personal data in the Ecuadorian criminal system, highlighting possible legal and operational limitations that hinder their adequate punishment, pointing out ambiguities in the classification of these crimes in the Comprehensive Organic Criminal Code and its weak connection with the Organic Law on Protection of Personal Data, among the most common crimes are unauthorized access to computer systems, identity theft, cyberstalking and fraud, The present study was conducted through qualitative and critical methods, review of legislation and jurisprudence evidencing regulatory gaps and insufficient enforcement of laws, which promotes impunity and exposes the victims, it is concluded that it is urgent to update the criminal system, to improve judicial resources and raise awareness among citizens to protect their personal data and encourage the reporting of cybercrimes.

Key words: Cybercrime; Data protection; Ecuadorian criminal system

RESUMO

O estudo examina os crimes cibernéticos e a proteção de dados pessoais no sistema penal equatoriano, destacando possíveis limitações legais e operacionais que impedem sua punição adequada, apontando ambiguidades na classificação desses crimes no Código Penal Integral Orgânico e sua fraca conexão com a Lei Orgânica de Proteção de Dados Pessoais, entre os crimes mais comuns estão o acesso não autorizado a sistemas de computador, roubo de identidade, cyberstalking e fraude, Esse estudo foi realizado com métodos qualitativos e críticos, uma revisão da legislação e da jurisprudência, revelando lacunas regulatórias e aplicação insuficiente das leis, o que promove a impunidade e expõe as vítimas.

Palavras-chave: Crimes cibernéticos; Proteção de dados; Sistema penal equatoriano

INTRODUCCIÓN

El avance de las tecnologías digitales ha transformado profundamente las dinámicas sociales, laborales y comerciales, generando nuevas oportunidades, pero también riesgos asociados a la vulnerabilidad en el ciberespacio. A nivel global, la digitalización ha propiciado la aparición de nuevas formas delictivas que afectan la integridad personal, el patrimonio y la privacidad de los ciudadanos (Escobar 2022)

En el contexto latinoamericano, la regulación de los ciberdelitos aún enfrenta desafíos significativos. La rápida evolución de las tecnologías y la globalización de las redes digitales dificultan la persecución efectiva de estos delitos, ya que muchos de ellos trascienden fronteras y dependen de marcos jurídicos que no siempre están armonizados entre países. En Ecuador, la tipificación de los delitos informáticos en el Código Orgánico Integral Penal (COIP) refleja un esfuerzo por regular estas conductas, pero persisten obstáculos en su tratamiento judicial (Geanfrank, 2022)

El COIP contempla delitos como el acceso no autorizado a sistemas informáticos, la suplantación de identidad y las estafas digitales. No obstante, la falta de denuncias, la dificultad para rastrear datos almacenados en servidores extranjeros y la ausencia de mecanismos claros de cooperación internacional han limitado la efectividad de las sanciones. Estas transgresiones, aunque tipificadas, presentan ambigüedades en la determinación de la culpabilidad y la aplicación de sanciones legítimas, lo que genera vacíos legales y altos índices de impunidad (Cabezas, 2023).

El problema jurídico central de este estudio radica en la efectividad del marco legal ecuatoriano para combatir los ciberdelitos, particularmente en lo que respecta a la protección de datos personales. El Art. 186 del COIP sanciona la suplantación de identidad con fines de estafa, mientras que el Art. 211 penaliza la alteración ilegal de identidad, especialmente cuando afecta a niños, niñas y adolescentes. Sin embargo, estos mecanismos resultan insuficientes ante la creciente sofisticación de los delitos informáticos y la facilidad con la que se vulneran los datos personales (Asamblea N. d., 2024)

En este contexto, la Ley Orgánica de Protección de Datos Personales establece directrices para la gestión y seguridad de la información, pero aún carece de mecanismos efectivos para garantizar su aplicación. La falta de claridad en la normativa y la escasa cultura de protección de datos en la ciudadanía incrementan el riesgo de que estos delitos continúen en aumento sin una respuesta penal adecuada (Asamblea N. d., 2021)

Volumen 8, No. 29, abril-junio 2025, ISSN: 2631-2735, https://revistalex.org

Ante este panorama, es fundamental fortalecer el marco legal ecuatoriano para asegurar la protección de los datos personales y la persecución efectiva de los ciberdelitos. Esto permitirá reducir la incidencia de estos delitos, garantizar la seguridad jurídica de los usuarios digitales y fomentar un entorno de mayor confianza en el uso de plataformas digitales.

Por lo tanto, el objetivo del estudio es examinar la legislación ecuatoriana sobre la penalización de los ciberdelitos, con énfasis en las sanciones establecidas en el Código Orgánico Integral Penal y su relación con la protección de datos personales en redes sociales y plataformas digitales. Asimismo, analizar la eficacia de las sanciones actuales e identificar las limitaciones y desafíos en la investigación y persecución de estos delitos en un contexto globalizado.

El estudio de los ciberdelitos y la protección de datos personales resulta fundamental debido a la creciente naturalización de estos delitos en la sociedad actual. Factores como la crisis económica y el desempleo han impulsado el aumento de fraudes, suplantaciones de identidad y otras actividades ilícitas en el entorno digital, afectando derechos fundamentales y la seguridad de los ciudadanos.

Esta investigación busca evaluar la eficacia de las sanciones penales vigentes y proponer mejoras al marco legal, garantizando la reparación de derechos y la prevención de futuros delitos informáticos. Se plantea la necesidad de establecer normativas claras y sin ambigüedades que permitan sancionar de manera efectiva estas conductas, evitando vacíos legales que desmotiven a la ciudadanía a denunciar. Asimismo, se propone fortalecer los mecanismos de cooperación internacional y actualizar la legislación para enfrentar los desafíos que plantea la cibercriminalidad en un entorno globalizado (Sálazar, 2021).

METODOLOGÍA

La investigación se desarrolló bajo un enfoque cualitativo, con un paradigma crítico-propositivo, permitiendo analizar la regulación de los ciberdelitos en el sistema penal ecuatoriano. Se emplearon métodos lógicos como la investigación documental y el análisis de legislación, los cuales facilitaron el discernimiento de ideas y la identificación de vacíos normativos en la penalización de estos delitos (Guevara, 2019).

Para el análisis de la normativa vigente, se recurrió al método descriptivo, mediante el cual se detallaron los conceptos fundamentales de los ciberdelitos, su tipificación en el Código Orgánico Integral Penal (COIP) y las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales (2021). Este método permitió exponer de manera clara y precisa las formas más comunes de ciberdelitos, como el acceso no autorizado a sistemas informáticos, la suplantación de identidad, el ciberacoso y las estafas digitales, entre otros (Asamblea N. d., 2024; Asamblea N. d., 2021).

Además, se examinó el contenido textual de la legislación penal sobre ciberdelitos y su aplicación en el sistema jurídico ecuatoriano, lo que facilitó la identificación de limitaciones en la persecución y sanción de estos delitos. A partir de este análisis, se plantearon propuestas orientadas a reformar el COIP con el fin de fortalecer la seguridad jurídica en el entorno digital y garantizar una mayor protección de los datos personales.

HALLAZGOS Y DISCUSIÓN

Ciberdelitos

Los ciberdelitos comprenden actividades ilícitas ejecutadas mediante tecnologías de la información y la comunicación (TIC). Su clasificación abarca diversas conductas, entre las que destacan el acceso no autorizado a bases de datos de instituciones públicas o privadas, vulnerando la información y los datos personales almacenados en estos sistemas (Astudillo, 2024,). También incluyen la suplantación de identidad y el ciberacoso, delitos que atentan contra la privacidad y seguridad de los datos personales.

Desde el ámbito jurídico, la protección de estos datos implica garantizar el derecho de los ciudadanos a decidir sobre su administración, acceso, publicación y modificación. En este sentido, los titulares de la información y los responsables de su tratamiento —incluyendo instituciones públicas, entidades bancarias y empresas de mensajería— tienen la obligación de resguardar la confidencialidad y seguridad de los datos personales (Ortiz, 2019).

Formas de ciberdelitos y su tipificación en el Código Orgánico Integral Penal (COIP)

Los ciberdelitos, también denominados delitos informáticos, se caracterizan por su comisión a través de las TIC con el propósito de llevar a cabo actividades ilícitas. En el contexto ecuatoriano, estas conductas están penalizadas en el Código Orgánico Integral Penal (COIP), el cual establece su tipificación y los criterios para determinar la antijuridicidad, la culpabilidad y el dolo en cada caso. La normativa busca definir con precisión la responsabilidad penal de los infractores y garantizar la aplicación de sanciones proporcionales a la gravedad de los delitos cometidos (Sálazar, 2021; Bazurto, 2024).

Entre los delitos informáticos contemplados en el COIP se incluyen el acceso no autorizado a sistemas informáticos, la alteración o manipulación de datos, la suplantación de identidad con fines fraudulentos, el ciberacoso y la difusión de contenido ilícito. La adecuada identificación y categorización de estas infracciones resulta esencial para fortalecer la seguridad digital y prevenir nuevos delitos en un entorno cada vez más interconectado.

Principales formas de ciberdelitos y su tipificación en el Código Orgánico Integral Penal (COIP)

Acceso no autorizado a sistemas informáticos, telemáticos o de telecomunicaciones

El Código Orgánico Integral Penal (COIP) establece que cualquier persona que acceda sin autorización a un sistema informático, telemático o de telecomunicaciones y permanezca en él contra la voluntad de sus legítimos administradores, con el propósito de copiar, alterar o eliminar información considerada sensible, será sancionada con una pena privativa de libertad de tres a cinco años (Asamblea N. d., 2024). No obstante, la normativa requiere mayor precisión respecto a la medición del daño causado y la posible imposición de sanciones pecuniarias o reparaciones civiles que compensen la vulneración de datos y los perjuicios generados por esta acción ilícita.

Supresión, alteración o suposición de identidad y estado civil

El COIP establece sanciones para quienes, de manera ilegal, alteren, añadan o supriman información relativa a la identidad propia o de terceros mediante el uso de programas informáticos o la manipulación de registros en documentos oficiales, como partidas de nacimiento, cédulas o bases de datos del Registro Civil. Este delito es castigado con penas privativas de libertad de uno a tres años.

Asimismo, si una persona registra como propio un hijo ajeno, suplanta la identidad de un menor o declara falsamente el fallecimiento de un recién nacido, la sanción se incrementa a tres a cinco años de prisión (Asamblea N. d., Código Orgánico Integral Penal, 2024).

Estafa en el ámbito digital

El COIP sanciona con penas de cinco a siete años de prisión a quienes, con el fin de obtener un beneficio económico indebido, induzcan a error a otra persona mediante la falsificación de hechos, la ocultación de información o la manipulación de sistemas digitales.

Se aplicará la pena máxima cuando el delito involucre:

1. El uso de tarjetas alteradas o dispositivos electrónicos fraudulentos.
2. La emisión de certificaciones falsas sobre operaciones.
3. La manipulación engañosa en la compra de valores.
4. La realización de transacciones ficticias.

Dado el impacto de estos delitos en la confianza digital y la seguridad financiera, el endurecimiento de las sanciones busca disuadir la proliferación de fraudes electrónicos en el entorno digital (Asamblea N. d., 2021).

Volumen 8, No. 29, abril-junio 2025, ISSN: 2631-2735, https://revistalex.org

Ciberacoso en plataformas digitales

El COIP tipifica el ciberacoso como un delito que involucra actos de naturaleza sexual cometidos a través de medios digitales, en los cuales una persona en posición de autoridad, utilizando amenazas o abuso de poder, busca intimidar o someter a otra persona.

Las sanciones contempladas incluyen:

- Uno a cinco años de prisión en casos generales.
- Tres a cinco años de prisión si la víctima es menor de edad, tiene discapacidad o se encuentra en situación de vulnerabilidad.
- Pena máxima si el agresor tiene un vínculo familiar o afectivo con la víctima.

Si el ciberacoso genera daños emocionales que conducen a la víctima a autolesionarse, la sanción se incrementará en un tercio. Además, si la conducta ocasiona perjuicios personales, laborales, educativos o patrimoniales, la pena también será aumentada.

Es fundamental que las investigaciones eviten la revictimización de las personas afectadas, garantizando que los procedimientos legales se lleven a cabo con el menor impacto posible en su integridad física y psicológica (Asamblea N. d., Código Orgánico Integral Penal, 2024).

Protección de datos personales en la legislación ecuatoriana

El análisis de la Ley Orgánica de Protección de Datos Personales (2021) y su articulación con el COIP revela la necesidad de fortalecer la seguridad jurídica en el entorno digital. Esta normativa establece los principios del tratamiento de datos personales y las obligaciones de los responsables de su manejo, con el objetivo de proteger la información de los ciudadanos.

Sin embargo, persisten vacíos normativos en relación con la tipificación y sanción de conductas que comprometen la seguridad de los datos personales, lo que representa una amenaza creciente en la era digital. Delitos como el robo de información, el fraude en línea y los ataques cibernéticos contra empresas y entidades públicas evidencian la necesidad de actualizar la legislación para garantizar una respuesta efectiva frente a los ciberdelitos (Rosas, 2022; Juca, 2023).

Clases de información que debe protegerse

Datos personales básicos

Los datos personales básicos comprenden información que permite la identificación directa de un individuo, tales como nombres, direcciones, números de identificación y cualquier otro dato que garantice su privacidad y discrecionalidad dentro de bases de datos públicas o privadas. La protección de estos datos es fundamental para salvaguardar la integridad de las personas, garantizando seguridad jurídica en su almacenamiento y tratamiento (Asamblea N. d., 2021; Tixi, 2023).

Datos sensibles

Los datos sensibles requieren un nivel de protección más alto debido a su potencial para causar discriminación o daño si son divulgados o manipulados indebidamente. Según el principio de necesidad, establecido en el Artículo 34 de la Constitución del Ecuador, la seguridad jurídica es un derecho irrenunciable de todos los ciudadanos y debe aplicarse especialmente en la protección de información biométrica, historial médico, orientación sexual, religión y creencias políticas. El tratamiento de estos datos debe regirse por estrictos criterios de confidencialidad y uso legítimo (Asamblea N. d., Constitución del Ecuador, 2008; Asamblea N. d., 2021).

Información financiera

La información financiera, que abarca cuentas bancarias, tarjetas de crédito, servicios de banca móvil y banca web, es considerada altamente sensible y está sujeta a protección legal. El sistema bancario,

Volumen 8, No. 29, abril-junio 2025, ISSN: 2631-2735, https://revistalex.org

cooperativista y financiero tiene la obligación de garantizar la seguridad de estos datos frente a posibles vulneraciones o fraudes. La divulgación o uso indebido de esta información puede facilitar la comisión de ciberdelitos, como fraudes electrónicos y robo de identidad (Silva, 2023).

Protección de los derechos del consumidor digital

El consumidor digital es aquel que adquiere bienes y servicios a través de plataformas tecnológicas y herramientas digitales. En este entorno, su información personal, como datos de contacto y preferencias de compra, debe ser protegida para evitar fraudes, publicidad engañosa o exposición indebida. La legislación ecuatoriana reconoce la necesidad de regular las transacciones digitales y brindar seguridad jurídica a los consumidores, asegurando que los productos adquiridos cumplan con estándares de calidad y que la información proporcionada en línea sea veraz y confiable (Pons, 2017).

Protección constitucional de datos personales

El Artículo 66, numeral 19 de la Constitución de la República del Ecuador garantiza el derecho a la protección de los datos personales. Esto incluye el acceso, la modificación y la decisión sobre su uso, procesamiento y difusión. Cualquier acción sobre estos datos debe contar con la autorización del titular y estar en conformidad con la normativa vigente, con el fin de evitar abusos o usos indebidos de la información personal (Asamblea N. d., Constitución del Ecuador, 2008)

Vacíos normativos y desafíos en la penalización de ciberdelitos

El marco legal ecuatoriano enfrenta múltiples limitaciones en la investigación y sanción de los ciberdelitos. La falta de claridad normativa, los desafíos transnacionales, las barreras técnicas y la escasez de recursos especializados dentro del sistema judicial dificultan la persecución efectiva de estos delitos. Además, el bajo nivel de denuncias, motivado por el desconocimiento normativo y la falta de sensibilización, contribuye a la impunidad de estas infracciones. Muchas personas no identifican la gravedad de los ciberdelitos, a pesar de que estos constituyen actos antijurídicos que pueden comprometer redes,

sistemas y datos sensibles. Este panorama evidencia que la legislación no evoluciona al mismo ritmo que las tecnologías de la información y comunicación (TIC), lo que hace que las sanciones penales actuales sean insuficientes para abordar estas nuevas formas delictivas (Ochoa, 2021; Acurio, 2020).

Se destaca la necesidad de reformar el Código Orgánico Integral Penal (COIP), armonizándolo con la Ley Orgánica de Protección de Datos Personales y la Ley de Comercio Electrónico. Estas reformas deberían contemplar:

- La creación de unidades especializadas en delitos informáticos dentro del sistema judicial.
- El desarrollo de estrategias de prevención y sensibilización ciudadana, promoviendo la denuncia de ciberdelitos.
- La tipificación más precisa de nuevas modalidades de delitos informáticos, adaptadas a la evolución tecnológica.

La ciberseguridad es un tema crítico para la protección digital de los ciudadanos y debe ser una prioridad estatal (Rico, 2022)

El principio de seguridad jurídica, consagrado en el Artículo 82 de la Constitución, establece la garantía de aplicación imparcial de las normas, evitando arbitrariedades. Este principio es clave en el contexto de los ciberdelitos, dada la rápida evolución de la tecnología y la creciente complejidad del entorno digital. Por ello, la actualización del marco normativo penal es esencial para asegurar sanciones eficaces, la reparación de derechos vulnerados y la adecuada protección de datos personales. Solo con una legislación moderna y efectiva se garantizarán los derechos de seguridad jurídica e integridad de los ciudadanos frente a las amenazas digitales (Asamblea N. d., Constitución del Ecuador, 2008; Sansó, 2017; Ordoñez, 2024).

La investigación sobre ciberdelitos y protección de datos personales en el sistema penal ecuatoriano se centra en la legislación vigente, con especial énfasis en las sanciones establecidas en el Código Orgánico Integral Penal (COIP) y su aplicación en redes sociales y plataformas digitales. Se evalúa la eficacia de estas sanciones, identificando limitaciones y desafíos en la investigación y persecución de delitos en

un contexto globalizado. Además, se examinan la Ley Orgánica de Protección de Datos Personales, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y el COIP, con el objetivo de determinar su efectividad en la penalización de delitos como estafas electrónicas, ciberacoso, acceso no autorizado a sistemas informáticos y suplantación de identidad.

Los hallazgos revelan avances y deficiencias dentro del marco normativo y operativo ecuatoriano. Si bien existen disposiciones para sancionar ciberdelitos, estas resultan insuficientes frente al crecimiento exponencial de las amenazas digitales. La falta de sanciones específicas y actualizadas limita la protección efectiva de los derechos fundamentales en el entorno digital y evidencia la necesidad de reformas legales. Es fundamental que el Estado garantice una protección adecuada de los datos personales y establezca sanciones más precisas y proporcionales a la gravedad de los delitos digitales. Solo mediante una legislación actualizada y una estrategia integral de prevención, detección y sanción se podrá combatir eficazmente los ciberdelitos, promoviendo un entorno digital seguro y justo para todos los ciudadanos (Acurio, 2020; Ortiz, 2019).

Discusión

El análisis legislativo sobre la aplicación de sanciones a ciberdelitos y la protección de datos personales en el sistema penal ecuatoriano revela vacíos normativos y desafíos operativos que afectan tanto el principio de seguridad jurídica de los ciudadanos como la capacidad del sistema judicial para enfrentar amenazas digitales (Contreras, 2024). La falta de precisión en la tipificación de delitos informáticos limita la efectividad de las sanciones y dificulta la protección de las víctimas. La ausencia de una estrategia penal actualizada permite que prácticas como el ciberacoso, el fraude en línea, la suplantación de identidad y el acceso no autorizado a sistemas informáticos persistan con altos niveles de impunidad, lo que evidencia la necesidad de una reforma integral del sistema judicial ecuatoriano (Tapia, 2021).

Las disposiciones del Código Orgánico Integral Penal (COIP) relacionadas con delitos informáticos presentan ambigüedades que obstaculizan su aplicación. Aunque el COIP regula delitos como el acceso ilícito a sistemas informáticos (Art. 234), la suplantación de identidad (Art. 211) y el ciberacoso (Art. 166) (Asamblea N. d., Constitución del Ecuador, 2008) la normativa no distingue entre conductas de distinta gravedad, lo que puede generar sanciones desproporcionadas o insuficientes. Además, la falta

de claridad dificulta que tanto instituciones como ciudadanos comprendan el alcance de las leyes, lo que reduce su efectividad en la prevención y persecución de ciberdelitos (Asamblea N. d., 2021).

Una desconexión crítica entre el COIP, la Ley Orgánica de Protección de Datos Personales y la Ley de Comercio Electrónico, Firmas y Mensajes de Datos también afecta la protección de los datos personales. Aunque esta última establece principios claros como el consentimiento informado y la confidencialidad, su aplicación en casos de ciberdelitos es limitada, ya que no existen mecanismos específicos para sancionar el uso indebido de datos personales en fraudes digitales o suplantación de identidad, dejando a las víctimas en una posición de vulnerabilidad (Asamblea, 2021). Este vacío normativo refleja una fragmentación en el marco legal penal que compromete el principio de seguridad jurídica.

Muchos ciudadanos optan por no denunciar ciberdelitos debido a la falta de garantías y sanciones efectivas. Esto no solo perpetúa la impunidad, sino que también expone a la población a un mayor riesgo de ser víctima de estas prácticas delictivas. La ausencia de un modelo sancionador adaptado a las nuevas infracciones penales digitales evidencia la ineficacia del sistema judicial ecuatoriano en este ámbito (Asamblea N. d., Código Orgánico Integral Penal, 2024; Congreso, 2002). En consecuencia, es fundamental desarrollar un marco normativo integral que permita enfrentar las amenazas digitales de manera efectiva, protegiendo los derechos digitales y fortaleciendo la seguridad jurídica de los ciudadanos.

A MANERA DE CONCLUSIÓN

El análisis del marco normativo ecuatoriano en materia de ciberdelitos evidencia la necesidad de reformas urgentes para fortalecer la protección de los ciudadanos en el entorno digital. El Código Orgánico Integral Penal (COIP) no aborda de manera adecuada delitos emergentes como el *ransomware* y el fraude con criptoactivos, lo que limita la capacidad de prevención y sanción. A pesar de la existencia de tipificaciones legales, su falta de precisión dificulta la aplicación efectiva de sanciones, lo que resalta la importancia de actualizar y clarificar las disposiciones normativas en función de los avances tecnológicos.

Volumen 8, No. 29, abril-junio 2025, ISSN: 2631-2735, https://revistalex.org

Si bien la Ley Orgánica de Protección de Datos Personales de 2021 establece principios fundamentales para la seguridad digital, su débil articulación con el COIP deja a las víctimas de delitos informáticos sin un marco integral de reparación y justicia. La ausencia de mecanismos sancionadores específicos para el uso indebido de datos personales en casos de fraude o suplantación de identidad incrementa la sensación de impunidad y vulnerabilidad ante los ciberdelincuentes, evidenciando la fragmentación normativa que afecta la protección de los derechos digitales.

Además, la escasez de recursos técnicos y la falta de unidades especializadas en delitos informáticos limitan la capacidad del sistema judicial para enfrentar estos delitos con eficacia. La formación insuficiente de operadores judiciales y la escasa sensibilización ciudadana sobre derechos digitales contribuyen a la baja tasa de denuncias, perpetuando la impunidad. Estas deficiencias subrayan la necesidad de una estrategia integral que combine reformas legales, inversión en recursos técnicos y campañas de concienciación ciudadana, garantizando así un entorno digital más seguro y una respuesta penal adecuada frente a las amenazas cibernéticas.

CONFLICTO DE INTERESES. Los autores declaran que no existe conflicto de intereses para la publicación del presente artículo científico.

REFERENCIAS

Acurio, D. P. (2020). Delitos informáticos en el Código Orgánico Integral Penal. Libertad.

Asamblea Nacional del Ecuador (1 de mayo de 2024). Código Orgánico Integral Penal. Sección Cuarta: Delitos contra la integridad sexual y reproductiva. Quito, Pichincha, Ecuador: Registro Oficial del Ecuador.

Asamblea Nacional del Ecuador. (20 de octubre de 2008). Constitución del Ecuador. Sección Octava: Trabajo y Seguridad Social. Quito, Pichincha, Ecuador: Registro Oficial del Ecuador.

Asamblea Nacional del Ecuador. (26 de mayo de 2021). Reglamento de la Ley Orgánica de Protección de Datos Personales. Ámbito de aplicación integral. Quito, Pichincha, Ecuador: Registro Oficial del Ecuador.

Asamblea Nacional del Ecuador (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial del Ecuador.

Astudillo, A. P.-A. (2024). Aplicación de la Ley Orgánica de Protección de Datos Personales en el sistema empresarial privado ecuatoriano. Revista de Investigación en Ciencias Jurídicas LEX, 7(25), 567-582. https://doi.org/10.33996/revistalex.v7i25.201

Bazurto, M. C. (2024). La ciberdelincuencia y la protección de datos personales. Sinergía Académica, 7(5), 594-612.

Cabezas, M. D.-A. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación española, con un enfoque de ciberseguridad y delitos informáticos. Universidad Politécnica Salesiana, 8(669), 2-43. https://www.ups.edu.ec/revistas-cientificas

Congreso Nacional del Ecuador (17 de abril de 2002). Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Principios Generales. Quito, Pichincha, Ecuador:

Registro Oficial del Ecuador.

Contreras, M. A.-A. (2024). Ciberacoso: una amenaza real para los jóvenes. Revista Debate Jurídico Ecuador. Revista Digital de Ciencias Jurídicas. UNIANDES, 7(2), 148-157. https://doi.org/10.61154/dje.v7i2.3513

Escobar, M. A. (2022). Análisis de ciberataques sobre el uso de redes sociales en relación con la protección de datos personales en Ecuador. Dominio de las Ciencias, 8(1), 1070-1079. http://dx.doi.org/10.23857/dc.v8i1.2622

Geanfrank, I. C.-A. (2022). Riesgos de seguridad de los datos en la web. Journal TechInnovation, 1(2), 43-49. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.43-49

Guevara, R. G. (2019). Propuestas metodológicas para la transformación en programas de posgrado desde el enfoque socioformativo. Atenas, 3(47), 105-114. https://www.redalyc.org/articulo.oa?id=478060102007

Juca, M. F. (2023). Ciberdelitos en Ecuador y su impacto social: Panorama actual y futuras perspectivas. Revista Científica Portal de la Ciencia, 4(3), 325-337. https://doi.org/10.51247/pdlc.v4i3.394

Ochoa, M. A.-A. (18 de febrero de 2021). Desafíos globales del cibercrimen. Maestría en Relaciones Internacionales. Quito, Pichincha, Ecuador: Universidad Andina Simón Bolívar.

Ordoñez, C. L. (2024). Marco legal de los delitos cibernéticos en Ecuador. Reincisol, 3(5), 1447-1469. https://doi.org/10.59282/reincisol.V3(5)1447-1469

Ortiz, C. N.-A. (2019). Normativa legal sobre delitos informáticos en Ecuador. Revista Científica Hallazgos, 4(1), 100-111. http://revistas.pucese.edu.ec/hallazgos21/

Pons, G. V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. Revista Latinoamericana de Estudios de Seguridad, V(20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Rico, C. M. (2022). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. Revista IUS, 7(31), 208-222. https://doi.org/10.35487/rius.v7i31.2013.27

Rosas, L. G. (2022). La protección de datos personales en Ecuador. Revista Internacional de Cultura Visual, 13(2), 2-16. https://doi.org/10.37467/revvisual.v10.4568

Sálazar, M. D. (2021). Dificultades en la investigación y persecución de cibercrímenes. Revista Científica de Ciencias Jurídicas, Criminología y Seguridad, 5(33), 8-62.

Sánchez, D. M.-A. (2023). Derecho a la protección de datos personales en la era digital. UNL.

Silva, V. D. (2 de septiembre de 2023). Protección jurídica del consumidor digital en la legislación ecuatoriana. Trabajo de titulación previo a la obtención del título de Abogado, Universidad Católica Santiago de Guayaquil. Guayaquil, Guayas, Ecuador: UCSG.

Tapia, H. E.-A. (2021). Importancia de la ciberseguridad y los derechos humanos. Misión Jurídica, 14(20), 142-158. https://doi.org/10.25058/1794600X.1912

Tixi, J. S. (2023). Delitos informáticos en el Código Orgánico Integral Penal ecuatoriano. Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas, VIII(1), 1610-1619. https://doi.org/10.35381/racji.v8i1.3339

ACERCA DE LOS AUTORES

Geovanna Gabriela Espinosa Carvajal. Lrofesora de educación primaria egresada del Instituto Pedagógico Camilo Gallegos. Licenciada en Secretariado Gerencial (ESPOCH). Ha participado en el Foro Acoso Político del Instituto de la democracia. Derecho y Perspectivas Jurídicas, derechos humanos y pueblos indígenas y derecho laboral. Especialista en prevención de drogas (Fundación EPRED). Tutor de proyectos de acogimiento infantil. Asistente Jurídica. Directora de asesorías asociadas.

Fernando Eduardo Paredes Fuentes. Licenciado en Ciencias políticas. Abogado de los Juzgados y Tribunales del Ecuador. Doctor en Jurisprudencia. Magister en Derecho Penal y Procesal Penal. Magister en Administración Educativa y Docencia Universitaria; Docente a tiempo completo de la Facultad de Jurisprudencia Ciencias Políticas y Económicas carrera de Derecho de la Universidad Tecnológica Indoamérica, Ecuador.