



Doi: <https://doi.org/10.70577/asce.v5i3.1106>

Recibido: 2026-08-27

Aceptado: 2026-09-10

Publicado: 2026-09-24

Ciberacoso en Ecuador: Un Análisis Crítico

Cyberbullying in Ecuador: A Critical Analysis

Autor(s)

Hermes Pedro Jiménez Pintado¹

Abogado

hermes.jimenez@funcionjudicial.gob.ec

<https://orcid.org/0009-0007-6417-3145>

Investigador independiente

Guayaquil - Ecuador

Raquel Iraida Jiménez Pintado²

Abogada

rjimenezp@ulvr.edu.ec

<https://orcid.org/0009-0006-6594-3343>

Universidad Laica Vicente Rocafuerte de Guayaquil

Guayaquil - Ecuador

Manuel Moisés Catota³

Abogado

mcatotac@ulvr.edu.ec

<https://orcid.org/0009-0003-0219-0354>

Universidad Laica Vicente Rocafuerte de Guayaquil

Guayaquil - Ecuador

Mickel Joel Culcay Conforme⁴

Abogado

mculcayc@ulvr.edu.ec

<https://orcid.org/0009-0006-5366-9770>

Universidad Laica Vicente Rocafuerte de Guayaquil

Guayaquil - Ecuador

Cómo citar

Jiménez Pintado, H. P., Jiménez Pintado, R. I., Catota, M. M., & Culcay Conforme, M. J. (2026). Ciberacoso en Ecuador: Un Análisis Crítico. *ASCE MAGAZINE*, 5(3), 3131–3147. <https://doi.org/10.70577/asce.v5i3.1106>



Resumen

La investigación analizó el tratamiento legal del ciberacoso. A través de una investigación basada en un análisis jurídico, con un enfoque cualitativo y análisis temático, con entrevistas semiestructurada a expertos en el área legal y técnica, se identifican debilidades en el Código Orgánico Integral Penal (COIP). Como la marcada falta de tipificación autónoma, y de acuerdo a los hallazgos se determina escasez de recursos tecnológicos y una percepción ciudadana de ineficacia en las sanciones actuales. Se concluye que no existe una tipificación autónoma del tipo penal, ni protocolos de educación digital obligatoria y la carencia de unidades de investigación especializada en el ámbito forense digital. Así como un marco regulatorio que exija a los prestadores de servicios digitales mayor transparencia y mecanismos de denuncia accesibles, que garanticen un equilibrio entre la libertad de expresión y el derecho a una existencia digital libre de agresiones y agravantes por anonimato.

Palabras clave: Derecho Penal; delito informático; Acoso sexual; Internet; Ciberdelito.



Abstract

This research analyzes the legal treatment of cyberbullying. Through a legal analysis using a qualitative approach, including interviews with legal and technical experts, weaknesses in the Comprehensive Organic Criminal Code (COIP) are identified. These include a marked lack of specific criminalization, a scarcity of technological resources, and a public perception of the ineffectiveness of current sanctions. The study concludes that reforms are needed to establish a specific criminal definition for cyberbullying, in addition to mandatory digital literacy protocols and the strengthening of specialized digital forensic investigation units. Furthermore, a regulatory framework is needed that requires greater transparency from digital service providers and accessible reporting mechanisms, guaranteeing a balance between freedom of expression and the right to a digital life free from harassment.

Keywords: Bullying; Internet; Cybercrime; Criminal Law; Computer Crime

Introducción

La revolución digital ha transformado la comunicación humana, pero también ha dado lugar a fenómenos perjudiciales como el ciberacoso, el cual afecta de manera desproporcionada a niños, niñas, adolescentes y mujeres jóvenes en Ecuador. El ciberacoso se distingue por el anonimato, la rápida viralización y la permanencia de los contenidos en la red, factores que intensifican el daño psicológico y social de las víctimas y crean nuevos escenarios de vulneración de derechos.

Según (Unicef, 2026) el Ciberacoso es una intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que busca atemorizar, enfadar o humillar a otras personas. Así como existen diferentes tipos de violencia, también hay varios ámbitos de violencia entre ellas la cibernética, que es la ejecutada, transmitida, comunicada a través de redes sociales, plataformas virtuales o cualquier otro medio tecnológico que incluye la publicación de videos, audios, o imágenes que vulneren el derecho a la intimidad, suplantación de identidad, vigilancia, acoso y hostigamiento virtual en todas sus formas, reclutamiento para llevar a cabo actos de violencia de género en contra de las mujeres, distribución de información personal de forma maliciosa, linchamiento cibernético entre otras (Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres, 2018).

Puede confundirse con el cyberbullying, que también es un nuevo tipo de persecución que se da por medio de las Tecnologías de la información y comunicación (TIC). Se lo puede definir como una agresión intencional y repetitiva, a través de medios electrónicos, por parte de un grupo o un individuo, contra una víctima, que no puede defenderse fácilmente (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2026). Se distingue entre Ciberacoso y *cyberbullying*, el primero se desarrolla entre desconocidos, adultos a menores o entre adultos, el segundo entre pares en ambientes educativos, aunque trascienda al entorno virtual. En cuanto a las sanciones también puede diferenciarse en el primero ya son sanciones penales mientras en el otro pueden ser protocolos educativos que busquen una medida socioeducativa.

Ambos delitos afectan el bien jurídico de la privacidad y reputación, y vulneran otros derechos fundamentales como la libertad de expresión y el derecho a una existencia sin violencia. Las víctimas se enfrentan con un ataque directo del victimario y en consecuencia a la ausencia de mecanismos judiciales eficaces que conlleven a una revictimización. Esto debilita la credibilidad

de las instituciones públicas, a que las víctimas prefieran no denunciar, lo cual genera la impunidad de los agresores en estos entornos virtuales.

Según datos de (Ecuador en Cifras , 2025) los hogares con uso de internet ascendieron en julio de 2025 a un 71,3% en los hogares. Mientras que el porcentaje de personas que utilizan internet es de 80,1%, para actividades comunicacionales y redes sociales. De allí surge la posibilidad de enfrentar riesgos y situaciones de violencia digital (Childfund, 2023).

Según Hinduja & Patchin, citado por (Pozo y otros, 2025) en los últimos años, la mayoría de los jóvenes se ha sentido atraídos por las redes sociales (como Instagram, TikTok y X), el chat de voz/texto en juegos populares (Roblox, League of Legends, Overwatch, PlayerUnknown Battlegrounds, Fortnite) y sitios de intercambio y transmisión de videos (como YouTube, Twitch y Live.Me). Esta tendencia ha llevado a un aumento en los informes de ciberacoso que ocurren en esos entornos y la desterritorialización del delito: el agresor puede estar en cualquier lugar.

Aunque el Código Orgánico Integral Penal (COIP) (2014) establece 14 tipos penales para delitos informáticos, el ciberacoso no aparece tipificado dentro de este marco legal. Se puede entender al ciberacoso, como la ejecución de actos despectivos y reiterados mediante el uso de tecnologías de la información, que provocan perjuicios palpables en quienes los sufren. Lo que conlleva a que la víctima se encuentre en un estado de indefensión jurídica y obstaculiza el ejercicio de su derecho a la tutela judicial efectiva. Por ello, resulta indispensable que el marco legal determine con precisión cuándo se vulneran estas garantías, las cuales están estrechamente vinculadas con otros derechos fundamentales como la privacidad, reputación, libertad de expresión y derecho a una vida libre de violencia.

Una de las características más visibles del ciberacoso en estos entornos es la rapidez con la que los contenidos pueden viralizarse, lo que permite que mensajes ofensivos, imágenes o rumores dañinos se difundan de manera masiva en pocos segundos. En este sentido, la (UNESCO, 2023) indica que “las redes sociales facilitan que el acoso trascienda las barreras físicas y temporales y su impacto se extienda a audiencias mucho más amplias” (p. 14).

El anonimato que ofrecen muchas veces estas plataformas virtuales actúa como intensificador de la violencia en estos entornos digitales. Diversas investigaciones han demostrado que la impunidad derivada de esta invisibilidad facilita que los agresores actúen con mayor frecuencia y niveles de violencia; La facilidad de ocultar datos de identificación en completa libertad, permite que naveguen sin ningún contratiempo, sin embargo, esta práctica genera complicaciones cuando se

trata de aplicar la norma frente a conductas ilícitas. El internet permite divulgar la información a gran cantidad de internautas, sin restricciones geográficas, pero, ese desarrollo, beneficioso en sus inicios, ha generado la proliferación de conductas inadecuadas.

La protección de datos en Ecuador se regula mediante la ley Orgánica de Protección de Datos Personales, esta tiene como objetivo salvaguardar el derecho fundamental a la protección de datos personales, otorgando a los individuos el control sobre su información y estableciendo un marco normativo que garantice el cumplimiento, por lo tanto, dentro de sus textos, regula los principios, derechos y obligaciones aplicables, así como los mecanismos de tutela necesarios para su protección (Molina y otros, 2025).

En este sentido, muchas plataformas en línea permiten la creación de cuentas únicamente con un correo electrónico, lo que facilita que los usuarios utilicen direcciones temporales o desechables para registrar cuentas con datos falsos pertenecientes a terceros o incluso inexistentes; esta práctica posibilita el uso de perfiles ficticios, a través de los cuales se pueden perpetrar diversos delitos que van desde el *cyberbullying* hasta delitos estafas u otras conductas ilícitas (Molina y otros, 2025).

Por ello es fundamental señalar las deficiencias regulatorias que aún persisten en materia tecnológica en diversas naciones que incluye a Ecuador. A diferencia de otros países donde se han establecido responsabilidades precisas para que las plataformas digitales supervisen y moderen sus contenidos, en otros países estos deberes legales continúan imprecisos y carecen de una definición clara.

A nivel global, el tratamiento del ciberacoso ha evolucionado a través de diversos marcos regulatorios y prácticas preventivas que sirven como referente para la legislación ecuatoriana.

- La Unión Europea, se destaca por tener marcos regulatorios actualizados, como la Directiva Europea sobre Derechos de las Víctimas, (UE) 2024/1385, adoptada en 2024, que garantiza protección integral y asistencia especializada a quienes sufren delitos en entornos virtuales.
- En Estados Unidos, la legislación ha dado pasos gigantescos para obligar a las instituciones educativas a establecer protocolos de actuación frente al ciberacoso, Los marcos legales en este país priorizan la educación preventiva y la responsabilidad de las escuelas y que las sanciones penales por sí solas no bastan para frenar la violencia digital (Gomez & Soto, 2025).

- En América Latina, ciertos países han promovido normativas para tipificar nuevas formas de delitos digitales. Ejemplos notables: (Ley 26904 Ley de Grooming Argentina, 2013) en Argentina, que incorporó el *grooming* como delito específico, y la Ley Olimpia (Gobierno de México, 2021), que sanciona la violencia digital y la difusión de contenido íntimo sin consentimiento.

Los estándares internacionales coinciden en la necesidad de tipificar el ciberacoso como un delito autónomo y en la urgencia de implementar políticas de sensibilización y ciudadanía digital.

La responsabilidad de los prestadores de servicios digitales o intermediarios tecnológicos, como las redes sociales y proveedores de internet, poseen un rol determinante tanto en la difusión como en el control del ciberacoso, debido a que proveen la infraestructura y cuentan con las herramientas técnicas (filtros y monitoreo) para intervenir (Barrero, 2021).

No obstante, la CEPAL advierte que la carencia de marcos regulatorios precisos ha dejado a los ciudadanos en una posición vulnerable, puesto que las empresas suelen anteponer sus beneficios económicos y la libertad de expresión a la seguridad de los usuarios.

A nivel comparativo, se observan distintos grados de avance:

- **Unión Europea:** Ha tomado la delantera con la Ley de Servicios Digitales, que impone a las plataformas la obligación de eliminar contenidos ilícitos con celeridad y proteger estrictamente a los menores.
- **América Latina y EE. UU.:** Persiste una controversia jurídica sobre cuánta responsabilidad deben asumir las empresas por lo que publican sus usuarios; la inacción en estos casos suele normalizar la violencia digital.
- **Ecuador:** El debate sobre los deberes legales de las plataformas tecnológicas frente al hostigamiento es todavía incipiente. A pesar de existir normas generales sobre delitos informáticos, no se han delimitado obligaciones específicas para que estos proveedores actúen preventivamente.

De allí la relevancia que Ecuador evolucione hacia un esquema de corresponsabilidad de los intermediarios digitales, donde se logre un equilibrio entre el respeto a los derechos fundamentales

y la implementación de mecanismos de denuncia efectivos que garanticen una tutela real para las víctimas.

Por tal razón resulta importante analizar el marco jurídico ecuatoriano frente al ciberacoso. Su tipificación en el COIP o las limitaciones para la protección de las víctimas. Por el cual se establece como objetivo general la identificación de los vacíos y cómo esta ausencia de tipificación compromete muchos derechos fundamentales de las víctimas y con la agravante cuando se comete de manera anónima. Se ha empleado un diseño de investigación con enfoque cualitativo y jurídico-dogmático, sustentado en el análisis de fuentes normativas y bibliográficas de alta relevancia, como el COIP y secundaria como las diferentes investigaciones de organizaciones internacionales, artículos científicos y toda información disponible en bases de datos como Google Scholar, scielo, web of science. Toda esta información se contrastará con entrevistas a expertos en el área para poder organizar y analizar resultados.

Revisión de los Delitos regulados en el Código Orgánico Integral Penal (2014) relacionados al ciberacoso: Aunque no existe la figura específica de ciberacoso, el sistema judicial utiliza los siguientes artículos para sancionar manifestaciones de violencia digital:

- **Grooming:** Sanciona el contacto con finalidad sexual con menores de edad a través de medios electrónicos (Art. 173).
- **Violación a la intimidad:** Castiga la difusión de información, datos o imágenes personales sin el consentimiento de la víctima (Art. 178).
- **Calumnia:** Se aplica cuando se realiza la imputación falsa de un delito a través de redes sociales o medios digitales (Art. 182).
- **Amenazas:** Regula la intimidación a una persona con causarle un mal, manifestada frecuentemente a través de mensajes o correos electrónicos (Art. 154).
- **Acoso sexual:** Aunque se enfoca en la persecución con fines sexuales, su segundo inciso hace referencia explícita al uso de tecnologías para configurar esta conducta (Art. 166).

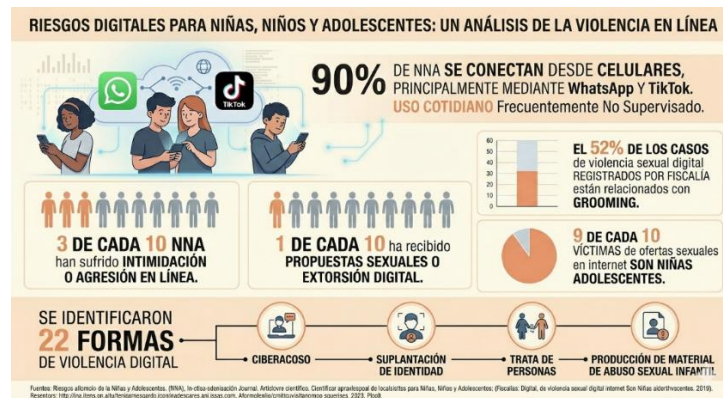
Cuáles son los vacíos legales dentro del COIP, La principal crítica a este cuerpo normativo es la falta de una tipificación independiente, por consiguiente, genera inseguridad jurídica e impunidad. Es decir, los aspectos no regulados o deficientemente tratados son:

- Al no encontrarse un artículo específico para el ciberacoso, conductas de hostigamiento sistemático que no tienen un fin sexual o de calumnia quedan a menudo fuera del alcance penal.
- Múltiples denuncias quedan desestimadas por no encuadrarse con un tipo penal existente.
- En Ecuador no se reguló sobre la responsabilidad de los prestadores de servicios (redes sociales, proveedores de internet) frente al ciberacoso.
- No existe un protocolo escolar de denuncia que estén articulados con el sistema judicial.
- Carencia de fiscalías especializadas en ciberdelitos y de laboratorios forenses con capacidad técnica para perseguir cuentas falsas o suplantaciones de identidad.

Por lo tanto, mientras que el COIP ofrece herramientas para casos de índole sexual o difamatoria, existe un vacío legal crítico para abordar el hostigamiento digital en todas sus dimensiones, lo que demanda una reforma urgente que tipifique el ciberacoso de forma autónoma.

Figura 1

Riesgos digitales en Niñas, niños y adolescentes en Ecuador



Fuente: *Childfun* (2025)

Nota. Infografía que detalla estadísticas de violencia digital y conectividad. Generada mediante el modelo de inteligencia artificial Gemini de Google (2026).

Material y métodos

Para la elaboración de este artículo científico, se empleó un diseño de investigación con enfoque cualitativo y jurídico-dogmático, sustentado en el análisis de fuentes normativas y bibliográficas de alta relevancia y entrevistas semi estructurada a dos (2) abogados y un (1) ingeniero experto en ciberseguridad, tomándose como criterio de selección la disponibilidad y la experticia en el área del Derecho Penal y Tecnológico.

Se emplearon herramientas tanto digitales como tradicionales para la recolección de datos, tales como agenda, procesador de palabras, Google drive, correos electrónicos, transcriptores con uso de IA como Turboscribe Transcription. Junto a lineamientos éticos para garantizar la transparencia mediante la aplicación de consentimientos informados a los entrevistados, detallando los objetivos y la metodología. Se priorizó la confidencialidad y protección de identidad a través de un sistema de codificación; por ejemplo, los nombres de los especialistas fueron sustituidos por los códigos Experto 1, 2 y 3. Adicional el acceso a la información recopilada está restringido al equipo investigador mediante equipos protegidos con contraseña que aseguren su uso exclusivo para fines académicos y científicos.

La validación del instrumento consistente en el guion de preguntas, se efectuó mediante juicio de expertos que analizo la suficiencia, claridad, coherencia y relevancia de cada pregunta, a través del índice de validez de contenido.

Tabla 1

Entrevistas abogados expertos

Preguntas de Entrevista	Experto 1	Experto 2
1.- Según su criterio considera que el ciberacoso está tipificado en el COIP?	No se encuentra tipificado como delito autónomo dentro del COIP	El artículo 166 del COIP tipifica el acoso sexual y su variante digital. El segundo inciso introduce las herramientas tecnológicas como agravante o medio de comisión (ciberacoso) con una sanción de 1 a 5 años, que esta conducta no constituye un delito separado en la legislación penal.
2.- Según su experiencia que	El ciberacoso no es un delito aislado, se vulneran	Hoy en día según investigaciones el ciberacoso se comete en su mayoría

derechos considera se ven vulnerados a las víctimas de ciberacoso?	derechos como la integridad psíquica y emocional, por la magnitud de la rapidez de difusión. También puede vulnerarse el derecho al buen nombre y honra, así como el derecho a la privacidad e intimidad.	contra niños, niñas y adolescente, La vulneración del principio del interés superior del niño, adicionalmente la ausencia de protocolos de respuesta inmediata por parte del Estado, lo que permite la revictimización, y la falta de seguridad jurídica a la integridad personal.
3.- ¿Según su criterio, cree que las penas contempladas en el COIP son suficientes para la gravedad de los delitos cibernéticos?	Las sanciones vigentes resultan insuficientes y desproporcionadas no contemplan agravantes específicos cuando estas conductas ocurren en entornos digitales.	No guardan proporción con la gravedad de los delitos cibernéticos. Es necesario fijar penas que se ajusten al daño real ocasionado.
4.- ¿Considera que el Estado ecuatoriano ha dotado a los órganos de administración de justicia de recursos forenses y personal técnico para abordar la complejidad probatoria de los delitos en entornos virtuales?	No existen fiscalías especializadas en ciberdelitos y los funcionarios no están capacitados para identificar el origen de cuentas falsas, correos electrónicos fraudulentos o números virtuales.	Manifiesta que el personal no está capacitado para identificar el origen de cuentas falsas, correos electrónicos fraudulentos o números virtuales, ni tampoco existen fiscalías especializadas en ciberdelitos.
5.- ¿Qué estrategias o reformas legales recomendaría implementar para mejorar la prevención y sanción del ciberacoso desde el ámbito jurídico?	La urgencia de establecer una tipificación autónoma del ciberacoso en el Código Orgánico Integral Penal (COIP), acompañada de un programa de formación técnica y legal permanente para jueces, fiscales y personal policial. Asimismo, enfatizó la necesidad de diseñar protocolos de denuncia precisos y fortalecer la colaboración con las empresas proveedoras de servicios digitales para garantizar la remoción inmediata de contenidos nocivo	Recomienda fortalecer las unidades especializadas como la UNASE, que ya han mostrado eficacia en delitos de secuestro mediante rastreo de llamadas y direcciones IP.

Elaborado por: *Jiménez et al (2026).*

Tabla 2*Entrevista a Ingeniero experto en Ciberseguridad*

Preguntas de Entrevista	Experto 3
1.- ¿según su criterio cuáles son las principales vulnerabilidades tecnológicas que facilitan el ciberacoso en el país?	El uso de plataformas digitales sin supervisión por parte de menores, con la insuficiente alfabetización digital, constituyen principales puntos críticos de vulnerabilidad. Estas deficiencias en la formación ciudadana facilitan la proliferación de perfiles ficticios y el robo de identidad, amparados en un anonimato que potencia la agresividad de los atacantes. Asimismo, se advierte que la carencia de mecanismos preventivos de seguridad en los equipos tecnológicos y las omisiones en el marco legal vigente generan un entorno propicio para que los agresores operen bajo un estado de impunidad, dificultando la protección efectiva de las víctimas y el rastreo técnico de los delitos.
2.- ¿Con el auge de la IA existen aplicaciones que ayuden a para prevenir o detectar el ciberacoso?	Existen las herramientas de seguridad integradas en redes sociales como Facebook, Instagram, TikTok y WhatsApp, las cuales permiten realizar bloqueos de usuarios, reportes de comportamiento y la gestión de la visibilidad de la información. Asimismo, es importante usar los sistemas de control parental como medida preventiva.
3.- ¿A que mecanismos efectivos de protección pueden acceder las víctimas?	En Ecuador, es posible denunciar en la Fiscalía General del Estado o ante la Policía Judicial y la Unidad de Ciberdelitos. También se recomienda la intervención de padres y docentes en casos de menores, así como el apoyo de organizaciones de asistencia legal y psicológica.
4.- ¿Qué otras estrategias de otros países se pueden tomar en cuenta para aplicar en Ecuador?	Campañas de educación digital desde edades tempranas, junto con protocolos escolares de respuesta inmediata, líneas telefónicas gratuitas y anónimas.

Elaborado por: *Jiménez et al (2026).*

La revisión bibliográfica Primaria, consistió en el Código Orgánico Integral Penal (COIP) de Ecuador. Este cuerpo legal constituye la norma matriz para examinar la respuesta punitiva del Estado frente a las conductas delictivas en el ciberespacio, que nos permitirá determinar si existe la tipificación de este delito en específico.

- Se analizaron artículos específicos del COIP que, aunque no tipifican el ciberacoso de forma autónoma, se utilizan para sancionar sus manifestaciones: Art. 173 (Grooming), Art. 178 (Violación a la intimidad), Art. 182 (Calumnia), Art. 154 (Amenazas) y Art. 166 (Acoso sexual).
- Complementariamente, se consultó la Constitución de la República del Ecuador (2008) para fundamentar la protección de derechos como el honor, privacidad, el buen nombre y la intimidad personal (Art. 66).

Métodos

Para contextualizar la magnitud social y los desafíos de regulación, se recurrió a informes de organismos especializados:

- **UNICEF:** Se utilizaron datos sobre la victimización global, identificándose que uno de cada tres adolescentes en el mundo ha sufrido acoso en línea. Asimismo, se consideraron sus recomendaciones para integrar la educación en ciudadanía digital en los sistemas escolares.
- **CEPAL:** este informe estudia el desafío de la regulación digital en América Latina, el cual concluye que la falta de normativas claras deja a los usuarios en situación de vulnerabilidad frente a las plataformas que priorizan la rentabilidad sobre la seguridad.
- **UNESCO y CHILDFUND:** recomiendan entornos de aprendizaje seguros y la necesidad de una guía multidisciplinaria que combine educación y marcos normativos que protejan a la niñez.

Así mismo artículos Científicos y Literatura Especializada, se seleccionó como investigaciones de impacto para profundizar en las causas y consecuencias del fenómeno, sobre la responsabilidad de los intermediarios de internet (Barrero, 2021), acoso escolar en Estados Unidos (Gomez & Soto, 2025), indicadores de la Tecnología e información (Ecuador en Cifras, 2025), la atención que

requiere Ecuador sobre el ciberacoso (Pozo y otros, 2025), la comparación con él (Gobierno de México, 2021) en cuanto a la ley Olimpia para el combate a la violencia digital y la (Ley 26904 Ley de Grooming Argentina, 2013).

Resultados

El análisis cualitativo de las entrevistas a expertos, Los hallazgos derivados del enfoque cualitativo, fundamentados en las entrevistas semiestructuradas realizadas a especialistas en las áreas jurídica y tecnológica, permiten identificar las brechas críticas en el tratamiento del ciberacoso en el Ecuador. A continuación, se detallan los resultados organizados por categorías temáticas:

1. Hay consenso entre los expertos a que el ciberacoso no está tipificado como delito autónomo. El artículo 166 del COIP regula una referencia normativa al sancionar el acoso sexual e incluir el uso de tecnologías en su segundo inciso, el análisis cualitativo realizado revela que esta disposición es limitada, ya que solo cubre conductas con fines sexuales y no el hostigamiento sistemático en otras esferas.
2. Los especialistas advierten que el ciberacoso vulnera una multiplicidad de derechos, entre ellos la integridad psíquica y emocional, el honor, el buen nombre y la intimidad personal. El análisis de las entrevistas subraya que la ausencia de protocolos de respuesta inmediata por parte del Estado facilita la revictimización de los afectados. Además, se enfatiza que la mayoría de las agresiones se dirigen contra niños, niñas y adolescentes, lo que conlleva la vulneración del principio del interés superior del niño y la seguridad jurídica.
3. Desde el ámbito pericial y judicial, existe una carencia de recursos humanos y tecnológicos. Existe consenso de los expertos sobre que no existen fiscalías especializadas exclusivas para ciberdelitos, lo que imposibilita la obtención de evidencia digital íntegra.
4. El experto en ciberseguridad señala como principales detonantes el uso sin supervisión de plataformas digitales por menores y la limitada alfabetización digital en la población. La invisibilidad y anonimato facilita la creación de perfiles ficticios que se catalogan como factores

que potencian la agresividad de los atacantes, permitiendo que los agresores operen bajo un estado de impunidad sistemática.

Discusión

El análisis cualitativo de las entrevistas revela una contradicción fundamental en el sistema penal ecuatoriano: mientras que la Constitución garantiza el derecho al honor, la privacidad y una vida libre de violencia, el (Código Orgánico Integral Penal, 2014) carece de una herramienta específica para proteger estas garantías en el entorno virtual.

El punto de debate es la insuficiencia del Artículo 166 del COIP. Aunque menciona el uso de tecnologías, lo hace dependiente del acoso sexual. Y deja fuera otras formas de hostigamiento metódico que no persiga un fin sexual, sino la humillación o el daño reputacional de la víctima.

En correspondencia con la CEPAL, la cuestión no debe limitarse a la sanción del agresor, sino ampliarse a la corresponsabilidad de los intermediarios digitales. Los expertos entrevistados subrayan que el enigma en las obligaciones de las plataformas para sofrenar contenidos y eliminar publicaciones agresivas refuerza la percepción de impunidad. Al contrastar esto con modelos como la Ley de Servicios Digitales de la Unión Europea, se evidencia que Ecuador se encuentra en una etapa incipiente, donde la falta de protocolos de retiro expedito de contenidos revictimiza a los afectados.

Finalmente, el análisis de las entrevistas pone de relieve que el ciberacoso no es solo un vacío legal, sino una deficiencia de infraestructura técnica. La ausencia de fiscalías especializadas y laboratorios forenses capaces de rastrear identidades digitales anónimas convierte a la normativa vigente en una "letra muerta" para la mayoría de las víctimas.

Conclusiones

Se concluye que el marco legal ecuatoriano actual es insuficiente para garantizar una tutela judicial efectiva frente al ciberacoso. Así como la comprobación de la vulneración de derechos fundamentales como la privacidad, reputación, libertad de expresión y el derecho a una existencia sin violencia a las víctimas. La falta de tipificación autónoma de este delito en el COIP, permite

que dichas conductas de hostigamiento queden impunes al no ajustarse exactamente a los tipos penales de acoso sexual o violación a la intimidad.

La investigación comprueba que la necesidad de una reforma al COIP que regule el ciberacoso como un delito específico junto con el anonimato y la viralización como agravantes. Es imperativo alinear la normativa nacional con estándares internacionales, como la Ley Olimpia de México o la Ley de Grooming de Argentina.

Se determina una carencia crítica de recursos forenses y de capacitación especializada a los operadores de justicia. Se debe fortalecer a la Policía judicial y la creación de fiscalías especializadas en ciberdelitos que cuenten con tecnología para rastreo de evidencias digitales.

Se recomienda la implementación obligatoria de programas de alfabetización y ciudadanía digital en el sistema educativo nacional, como la herramienta educativa más eficaz para prevenir la violencia digital desde etapas tempranas.

Finalmente, es necesario avanzar hacia un marco regulatorio que exija a los prestadores de servicios digitales mayor transparencia y mecanismos de denuncia accesibles, que garanticen un equilibrio entre la libertad de expresión y el derecho a una existencia digital libre de agresiones.

Referencias bibliográficas

- Barrero, A. (2021). Responsabilidad de los intermediarios de internet en el derecho de la UE. *Revista Española de Derecho Constitucional*, 107-132. <https://doi.org/https://doi.org/10.18042/cepc/redc.123.04>
- Childfun. (27 de Junio de 2025). *Niñas, niños y adolescentes en Ecuador enfrentan 22 formas de violencia digital, revela investigación de Childfun*. <https://www.childfund.ec/ninas-ninos-y-adolescentes-en-ecuador-enfrentan-22-formas-de-violencia-digital-revela-investigacion-de-childfund/>
- Childfund. (2023). *Campaña “Naveguemos Seguros”*. <https://www.eloriente.com/articulo/childfund-presento-en-ecuador-la-campa>
- Código Orgánico Integral Penal. (2014). *Registro Oficial Suplemento 180 - 10-02-2014*. Lexis.



- Ecuador en Cifras . (23 de abril de 2025). *Indicadores de tecnología de la información y educación*.
<https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/>
- Gobierno de México. (26 de Abril de 2021). *La “Ley Olimpia” y el combate a la violencia digital*.
<https://www.gob.mx/profeco/articulos/la-ley-olimpia-y-el-combate-a-la-violencia-digital?idiom=es>
- Gomez, M., & Soto, L. (12 de Diciembre de 2025). *Acoso escolar (bullying) en los Estados Unidos: qué dice la ley*. <https://www.abogado.com/recursos/derechos-civiles/acoso-en-las-escuelas-y-c-mo-lo-protege-la-le.html>
- Google Gemini. (4 de Marzo de 2026). *Infografía sobre riesgos digitales para niñas, niños y adolescentes [Imagen generada por IA]*. <https://gemini.google.com/>
<https://gemini.google.com/>
- Ley 26904 Ley de Grooming Argentina. (2013). Buenos Aires, Argentina.
- Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres. (2018). Ecuador.
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (26 de Febrero de 2026).
<https://www.telecomunicaciones.gob.ec/conoce-mas-ciberacoso/>
- Molina, K., Mendoza, S., & Espinoza, J. (2025). La frontera entre privacidad y evasión de responsabilidad: anonimato en. *Religación*, 1-14.
- Pozo, C., Mendez, C., Sandoval, D., & Atencio, R. (2025). Ciberacoso: Realidad que requiere atención en Ecuador. *Universidad & Sociedad*, 17(3).
- UNESCO. (2023). *Cyberbullying: Ending violence in and through digital spaces*.
<https://unesdoc.unesco.org/>
- Unicef. (18 de Enero de 2026). *Ciberacoso: qué es y cómo detenerlo*. <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo>

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.