UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE DERECHO

TIPIFICACIÓN Y RESPUESTA PENAL AL CIBER ACOSO EN ECUADOR: ANÁLISIS CRÍTICO DEL COIP Y SUS BRECHAS NORMATIVAS

Trabajo de titulación previó a la obtención del
Título de Abogado.

AUTORES: ADRIÁN WILSON PARALES QUINTO Y
ELVIS DAVID MUÑOZ FAJARDO

TUTOR: ABG. MGRT. MARCOS FRANCISCO MOREIRA ARGUDO.

GUAYAQUIL -ECUADOR 2026

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Adrian Wilson Parrales Quinto con documento de identificación N° 0941061517 y Elvis David Muñoz Fajardo con documento de identificación N° 0911218196; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 6 de febrero del año 2026

Atentamente,

Adrian Wilson Parrales Quinto
0941061517

Elvis David Muñoz Fajardo
0911218196

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Adrian Wilson Parrales Quinto con documento de identificación No. 0941061517 y Elvis David Muñoz Fajardo con documento de identificación No. 0911218196, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Ensayo o Articulo Académico: "Tipificación Y Respuesta Penal Al Ciber Acoso En El Ecuador: Análisis Crítico Del Coip Y Sus Brechas Normativas", el cual ha sido desarrollado para optar por el título de: Abogado, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 6 de febrero del año 2026

Atentamente,

Adrian Wilson Parrales Quinto
0941061517

Elvis David Muñoz Fajardo
0911218196

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Marcos Francisco Moreira Argudo con documento de identificación N° 0911023406 docente de la Universidad Politécnica Salesiana , declaro que bajo mi tutoría fue desarrollado el trabajo de titulación "Tipificación Y Respuesta Penal Al Ciber Acoso En El Ecuador: Análisis Crítico Del Coip Y Sus Brechas Normativas", realizado por Adrian Wilson Parrales Quinto con documento de identificación N° 0941061517 y por Elvis David Muñoz Fajardo con documento de identificación N° 0911218196, obteniendo como resultado final el trabajo de titulación bajo la opción Ensayo o Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 6 de febrero del año 2026

Atentamente,

Marcos Francisco Moreira Argudo
0911023406

RESUMEN:

El presente artículo realiza un análisis jurídico–crítico del tratamiento penal del ciberacoso en el ordenamiento jurídico ecuatoriano, a partir de la constatación de que el Código Orgánico Integral Penal (COIP) no contempla un tipo penal autónomo que regule de manera integral el hostigamiento digital reiterado. Esta ausencia normativa resulta especialmente problemática en un contexto social caracterizado por el uso masivo de tecnologías de la información y comunicación, donde las conductas de acoso en entornos digitales generan afectaciones graves y prolongadas a la integridad psíquica, la dignidad, la honra y la tranquilidad personal de las víctimas.

Desde una metodología cualitativa, de carácter documental y dogmático, la investigación examina las disposiciones del COIP actualmente aplicables a conductas de acoso digital —como el hostigamiento por medios tecnológicos, la violencia psicológica, la violación a la intimidad y la difusión indebida de información—, identificando las dificultades de subsunción típica y la fragmentación normativa que impiden una respuesta penal eficaz frente al ciberacoso no necesariamente sexual. El análisis se complementa con un estudio de los derechos constitucionales comprometidos, en particular la integridad psíquica, la honra, la intimidad y la protección de datos personales, evidenciando una desarmonización entre el marco constitucional y la legislación penal vigente.

Asimismo, el artículo incorpora un análisis de derecho comparado, examinando las respuestas normativas adoptadas en países como España,

México, Colombia y Chile, con el fin de identificar modelos de tipificación, agravantes digitales y mecanismos de protección que permitan enfrentar de manera más adecuada el fenómeno del hostigamiento digital reiterado. A partir de este examen, se constata que la utilización de figuras penales tradicionales, diseñadas para contextos analógicos, resulta insuficiente para abarcar la complejidad del ciberacoso en entornos digitales.

Finalmente, el trabajo propone lineamientos de reforma al COIP orientados a la incorporación de un tipo penal autónomo de ciberacoso, acompañado de agravantes específicas y medidas cautelares digitales, con el objetivo de fortalecer la protección penal de las víctimas, garantizar el principio de legalidad y asegurar una respuesta coherente y proporcional del sistema penal ecuatoriano frente a las nuevas formas de violencia digital.

PALABRAS CLAVE: Ciberacoso, Acoso escolar, Violencia digital, Código Orgánico Integral Penal (COIP), Vacíos normativos, Derecho penal ecuatoriano, Acoso tecnológico, Protección de víctimas, Legislación comparada, Tipificación penal, Brechas jurídicas, Adolescencia y redes sociales, Uso de internet en Ecuador, Hostigamiento digital, Reforma penal.

ABSTRACT:

This article presents a legal-critical analysis of the criminal treatment of cyberbullying in the Ecuadorian legal system, based on the observation that the Comprehensive Organic Criminal Code (COIP) does not include an autonomous criminal offense that comprehensively regulates repeated digital harassment. This **regulatory** gap is particularly problematic in a social context characterized by the widespread use of information and communication technologies, where harassment in digital environments causes serious and prolonged harm to the psychological integrity, dignity, honor, and personal peace of mind of the victims.

Using a qualitative, documentary, and dogmatic methodology, the research examines the provisions of the COIP currently applicable to digital harassment—such as harassment by technological means, psychological violence, violation of privacy, and improper dissemination of information—identifying the difficulties in legal classification and the fragmented regulations that hinder an effective criminal response to cyberbullying that is not necessarily sexual in nature. The analysis is complemented by a study of the constitutional rights at stake, particularly psychological integrity, honor, privacy, and the protection of personal data, revealing a disconnect between the constitutional framework and current criminal legislation.

The article also incorporates a comparative law analysis, examining the legal responses adopted in countries such as Spain, Mexico, Colombia, and Chile, in order to identify models of criminalization, digital aggravating factors, and protection mechanisms that allow for a more effective response

to the phenomenon of repeated digital harassment. This examination confirms that the use of traditional criminal offenses, designed for analog contexts, is insufficient to encompass the complexity of cyberbullying in digital environments.

Finally, the work proposes reform guidelines for the Comprehensive Organic Criminal Code (COIP) aimed at incorporating an autonomous criminal offense of cyberbullying, accompanied by specific aggravating factors and digital precautionary measures, with the objective of strengthening the criminal protection of victims, guaranteeing the principle of legality, and ensuring a coherent and proportionate response from the Ecuadorian criminal justice system to new forms of digital violence.

Keywords:

Cyberbullying, School bullying, Digital violence, Comprehensive Organic Criminal Code (COIP), Regulatory gaps, Ecuadorian criminal law, Technological harassment, Protection of victims, Comparative legislation, Criminal classification, Legal gaps, Adolescence and social networks, Internet use in Ecuador, Digital harassment, Criminal reform.

DEDICATORIA

Con el corazón lleno de gratitud, este trabajo se lo dedico en especial a mis ángeles que me cuidan desde el cielo, y que eh sentido su presencia en todo momento. A lo largo de este camino universitario e sentido su presencia desde lo más alto, también dedicarle a mi mama la Ing. Mayra Quinto por su apoyo incondicional y por ser mi pilar en este trayecto de mi vida, también dedicarle este trabajo a mi papa el Abg. Wilson Parrales por sus enseñanzas y consejos que me supo dar para poder resolver cualquier circunstancia en mi trayecto académico.

También le dedico este trabajo a mi familia que sin duda han estado para mí en todo momento, me han acompañado y preguntándome que tal me va en la universidad, también dedicarle el trabajo a Dios porque sin él no sería nada de esto posible, por brindarme salud, bienestar, inteligencia y sobre todo humildad.

Dedico este trabajo también a mis amistades y hermanos de diferente sangre por apoyarme y darme de una u otra forma una palabra de aliento, para yo no rendirme y asi poder seguir afrontando cada desafío que se venía presentando, también a la persona que Dios puso en mi camino para que cogido de la mano de ella sepa superar cualquier obstáculo, sin más nada que decir dedico este trabajo a todas las personas que estuvieron pendiente de mi crecimiento personal y profesional a lo largo de estos cuatro años.

Adrian Wilson Parrales Quinto.

AGRADECIMIENTO

Quiero iniciando este agradecimiento a Dios en primer lugar y también a la madre santísima que me a protegido y cubierto con su manto poderoso, además de saberme guiar cuando me sentía totalmente perdido, y me ayudaron a encontrar una salida de ese túnel sin salida en que muchas veces me encontraba.

También quiero agradecerle a la vida por ponerme en el lugar que estoy y por haber encontrados amistades muy buenas y profesionales muy sobresalientes, además agradecer a las personas que me brindaron por primera vez un espacio para yo poderme desempeñar en mi área de estudio como un profesional.

Agradezco también a mis compañeros y amigos de aula que comenzamos todo este camino juntos hace cuatro años atrás y en especial a los que siguieron y no se rindieron nunca, también a los que se quedaron en el camino que de una u otra forma, llegaron hacer parte esencial de mi vida universitaria.

Además, agradecer siempre a las personas que confiaron en mi y lo siguen haciendo, les agradezco de todo corazón por haber formado parte de esta etapa de mi vida, así que le agradezco mucho a cada una de las personas que menciono en brevedad en este trabajo.

Adrian Wilson Parrales Quinto.

TABLA DE CONTENIDO

INTRODUCCIÓN

El desarrollo acelerado de las tecnologías de información y comunicación (TIC) ha generado nuevas dinámicas sociales y jurídicas. Una de las manifestaciones más preocupantes es el ciberacoso, entendido como el hostigamiento reiterado mediante plataformas digitales, capaz de producir daños psicológicos, emocionales y sociales. La literatura jurídica y psicológica coincide en que esta forma de violencia vulnera derechos fundamentales como la dignidad, la integridad personal y la intimidad, y que afecta especialmente a mujeres, niñas, niños y adolescentes.

En Ecuador, pese a la creciente incidencia del ciberacoso, el Código Orgánico Integral Penal (COIP) no contempla un tipo penal autónomo que regule estas conductas, lo que ha generado vacíos en la aplicación de justicia, inseguridad jurídica y desprotección para las víctimas. Investigaciones recientes sostienen que la ausencia de una definición penal clara obstaculiza la persecución penal y vulnera el principio de legalidad; (Barreto, 2024).

Con el fin de aportar al debate legislativo y jurídico, este estudio realiza un análisis crítico del tratamiento penal del ciberacoso en Ecuador y compara su regulación con la de otros países como España, México, Colombia y Chile. A través de una metodología cualitativa y documental, se identifican brechas normativas y se proponen reformas orientadas a modernizar el sistema penal ecuatoriano en consonancia con estándares internacionales de derechos humanos.

Asimismo, se recomienda incorporar medidas cautelares digitales como la eliminación obligatoria de contenido, el bloqueo preventivo de perfiles, la prohibición de contacto digital y la protección reforzada de datos personales. Estas medidas se consideran fundamentales para

impedir la repetición del daño, pues la naturaleza viral de las plataformas digitales hace que los efectos del ciberacoso sean inmediatos, amplificados y frecuentemente irreversibles.

El artículo concluye que Ecuador requiere modernizar su legislación penal para enfrentar los desafíos del entorno tecnológico actual. La ausencia de un tipo penal específico de ciberacoso no solo limita la capacidad operativa del sistema de justicia, sino que deja en estado de vulnerabilidad a grupos especialmente expuestos como niños, adolescentes, mujeres y minorías. La propuesta basada en el modelo colombiano ofrece un camino viable para desarrollar una respuesta penal clara, proporcional y acorde con los estándares internacionales de protección digital. El fortalecimiento del COIP mediante la incorporación de una figura penal autónoma, medidas cautelares efectivas y un enfoque preventivo permitiría al Estado ecuatoriano cumplir con sus obligaciones constitucionales de proteger la integridad, la dignidad y los derechos digitales de sus ciudadanos frente a la violencia contemporánea del ciberespacio.

PROBLEMA DE ESTUDIO

El presente artículo aborda el siguiente problema central:

¿La ausencia de un tipo penal autónomo de ciberacoso en el Código Orgánico Integral Penal (COIP) genera un déficit de protección penal y dificultades de subsunción típica que afectan el principio de legalidad y el acceso a la justicia de las víctimas, en comparación con modelos de tipificación y/o medidas de protección existentes en el derecho comparado?

Este problema se formula desde una perspectiva estrictamente jurídico–penal, centrada en la coherencia del sistema normativo y en la capacidad del COIP para responder de manera adecuada al fenómeno del ciberacoso no necesariamente sexual. El análisis se enfoca en determinar si la actual regulación fragmentada permite una subsunción típica conforme al principio de legalidad y si garantiza un acceso efectivo a la justicia, tomando como referencia experiencias comparadas que han optado por tipificaciones específicas o por mecanismos de protección más definidos.

Este problema nace del hecho de que el Ecuador no cuenta con un delito autónomo de "ciberacoso", sino que las conductas se procesan mediante figuras aisladas del COIP tales como: Hostigamiento por medios tecnológicos (ART. 154.2 COIP, 2014), introducido por la Ley Orgánica Reformatoria del COIP para Prevenir y Combatir la Violencia Sexual Digital (R.O. 526, 2021), aplicable únicamente cuando exista intención de causar daño a la integridad física, psíquica, emocional o dignidad personal.

El art. 154.2 COIP, introducido por la reforma 526 de 2021 sobre violencia sexual digital, sanciona el hostigamiento por medios tecnológicos cuando:

- Existe búsqueda de cercanía,
- A través de medios tecnológicos o digitales,

- Con la finalidad de causar daño a la integridad física, psíquica, emocional o dignidad personal de la víctima.

Violencia psicológica (ART. 157 COIP, 2014)aplicable solo en relaciones familiares o contra la mujer.

Violación a la intimidad, revelación de datos o difusión de información restringida (arts. 178, 180, 229 COIP).

Delitos sexuales cometidos mediante medios electrónicos (ARTS. 173 & 174 COIP, 2014) Calumnia o injuria por medios electrónicos (art. 182 COIP y artículos correlativos).

El **ciberacoso típico**, tal como se manifiesta en la realidad social y digital, **no siempre tiene finalidad física ni sexual**, sino que produce:

- daño psíquico,
- humillación pública,
- control emocional,
- intimidación sostenida,
- afectación a la dignidad y tranquilidad personal.

Esto genera una respuesta penal fragmentada, donde conductas reiteradas de hostigamiento digital como humillaciones públicas, amenazas no físicas, manipulación emocional en línea, difusión de contenido no íntimo pero perjudicial, ciberburling y campañas digitales de odio pueden no encajar adecuadamente en ninguna figura penal existente.

El problema de fondo consiste en determinar si esta fragmentación vulnera:

1. El principio de legalidad y taxatividad penal,

2. El derecho a la integridad psíquica,

3. El derecho a la protección de datos personales,

4. La honra y reputación, y

5. El acceso a la justicia.

La contextualización normativa del problema, el problema se agrava porque, a nivel constitucional:

-La Constitución garantiza la integridad física, psíquica, moral y sexual, protege la honra, reputación e intimidad y reconoce el derecho a la protección de datos personales. (CRE, 2008).

Todos son derechos directamente afectados por el ciberacoso, pese a ello, el COIP no ha desarrollado un tipo penal que abarque integralmente el acoso digital, a pesar de que sí reguló otras conductas digitales como:

- Contacto sexual por medios electrónicos con menores, hostigamiento digital con finalidad sexual, violación a la intimidad mediante tecnologías, revelación ilegal de bases de datos (COIP).
- Diversos autores ecuatorianos han señalado que el COIP no es suficiente para enfrentar el ciberacoso como fenómeno complejo, reiterado y digital.
- Pozo Chugá (2025), en Ciberacoso: análisis del COIP y sus limitaciones (SciELO), concluye que "el ciberacoso no se encuentra tipificado de manera específica, lo que provoca dispersión normativa y dificultades para su judicialización". Esto sustenta la premisa de que el problema es real y reconocido en la literatura científica.
- Zuñiga Vásquez (2021), Ciberacoso, cyberbullying y principio de legalidad (UNIANDES), plantea que la ausencia de un tipo penal autónomo genera inseguridad jurídica e incumplimiento del principio de taxatividad penal, ya que el acoso digital se persigue mediante figuras colaterales del COIP.

Violencia digital y políticas públicas

El Protocolo de Violencia Digital del Ministerio de Educación (2023) reconoce el ciberacoso como una forma de violencia que afecta a niñas, niños y adolescentes en contextos

escolares.

- Lo relevante es que el Estado reconoce el problema, pero no existe una figura penal integral. La Ley Orgánica para Prevenir y Erradicar la Violencia contra las Mujeres (2018) reconoce la violencia digital, pero no genera un tipo penal, dejando el área penal sin armonización normativa. Intentos legislativos específicos

El Proyecto de Ley para Prevenir la Violencia, el Acoso Digital y la Violación a la Intimidad (Montaño, 2020) proponía la creación del delito 175.2 "Ciberacoso sexual". Aunque no fue aprobado íntegramente, muestra que el legislativo detectó el vacío normativo.

Perspectiva comunicacional y derechos digitales

El Consejo de Comunicación (2020), en el artículo "Acoso cibernético perspectivas post- COVID-19", afirma que el acoso digital requiere tipificaciones más claras, pues actualmente se judicializa desde delitos como el hostigamiento, revelación de datos, violación a la intimidad y otros.

Problema específico a investigar

Del análisis anterior podemos observar que existe una brecha normativa en el COIP respecto de la tipificación del ciberacoso, ya que el ordenamiento penal carece de un tipo penal autónomo que abarque de manera integral el hostigamiento digital no sexual, reiterado y potencialmente dañino, lo cual genera inseguridad jurídica, dificultades probatorias, protección diferenciada según el tipo de víctima y dispersión entre varias figuras penales incompletas.

Este problema se ve reforzado por:

- La fragmentación normativa (arts. 154.2, 157, 173, 174, 178, 180, 229 COIP),
- La desarmonización con la Constitución (arts. 66.3, 66.8, 66.19 CRE),
- La evidencia científica que muestra la insuficiencia del marco jurídico (Pozo Chugá, Zuñiga, Vicuña-Pozo, Consejo de Comunicación),
- y los intentos legislativos fallidos por crear tipos de ciberacoso (Proyecto Montaño, 2020).

Este artículo científico es relevante porque:

- El ciberacoso constituye un fenómeno creciente, especialmente entre adolescentes y mujeres, según el Ministerio de Educación (2023) y el Consejo de Comunicación (2020).
- La falta de tipificación afecta el acceso a la justicia porque muchas denuncias no prosperan al no encajar en tipos penales existentes.
- La respuesta penal actual puede vulnerar el principio de legalidad, porque se "fuerzan" tipos que no fueron creados para abarcar el fenómeno digital.
- El Ecuador tiene una obligación constitucional de proteger la integridad psíquica, la honra y los datos personales (ARTS.66.3&66.8&66.19CRE, 2008).
- El análisis comparado sugiere que otros países (ej. Colombia, España, Chile) ya han avanzado hacia la tipificación, mientras que Ecuador mantiene vacíos. 6. Conclusión provisional para el problema de estudio

El artículo científico analizará cómo la falta de un tipo penal autónomo de ciberacoso en Ecuador genera inconsistencias normativas, insuficiencias de protección, inseguridad jurídica y dispersión entre tipos penales parciales, a la luz de la doctrina, la experiencia legislativa reciente y los estándares constitucionales y de derechos digitales.

Esta falta de coherencia entre el marco constitucional y el marco penal es uno de los ejes del problema de investigación

JUSTIFICACIÓN

El ciberacoso constituye una problemática creciente en Ecuador, especialmente entre jóvenes y adolescentes. Según el archivo adjunto:

- Uno de cada cinco estudiantes ha sido víctima de acoso escolar.

- Entre las formas más comunes de agresión aparece el ciberacoso, junto con insultos, rumores y sustracción de pertenencias.
- La violencia digital tiene efectos psicológicos severos, puede convertirse en un hostigamiento permanente gracias a la disponibilidad tecnológica y, en casos extremos, puede conducir a daños irreparables.

A pesar de este contexto, el COIP no tipifica directamente el ciberacoso, lo que obliga a fiscales, jueces y víctimas a encajar estos hechos en tipos penales tradicionales (hostigamiento, violación de intimidad, amenazas, violencia psicológica), generando ambigüedad, impunidad y respuestas insuficientes.

La investigación de este artículo científico es necesaria porque:

- Existe un vacío normativo que vulnera derechos constitucionales como integridad, dignidad, intimidad y seguridad.
- Actualmente las víctimas, fiscales y jueces deben "forzar" los hechos de ciberacoso dentro de tipos tradicionales, generando **ambigüedad, desprotección e impunidad**, tal como advierte el *Consejo de Comunicación (2020)* en su estudio sobre acoso cibernético.
- El uso masivo de internet exige que la legislación penal se adapte al entorno digital.
- La digitalización convierte el acoso en una conducta *permanente, anónima, multicanal y difícil de detener*, lo cual exige respuestas penales especializadas.
- El legislador ecuatoriano carece de herramientas modernas para sancionar conductas presentes en otros ordenamientos. Ni los arts. 154.2 ni 157 del COIP abarcan todo el espectro del ciberacoso: el primero exige intención de dañar integridad física o sexual, y el segundo se limita a relaciones familiares o violencia de género.
- Por ello, resulta imprescindible un análisis crítico del COIP y la formulación de propuestas que permitan proteger de manera eficaz a las víctimas y garantizar una adecuada

respuesta penal.

Este artículo científico es relevante porque se analiza el fenómeno desde un enfoque interdisciplinario:

- Derecho penal, derechos fundamentales, protección de datos, sociología digital y política criminal.
- Integra fuentes normativas, jurisprudenciales y doctrinarias, siguiendo la estructura recomendada para estudios jurídicos de alto nivel.
- Lagunas que afectan procedimientos penales: Los operadores de justicia carecen de herramientas claras para: identificar patrones de hostigamiento digital, valorar pruebas electrónicas, establecer continuidad delictiva, y determinar agravantes tecnológicas.
- Efectos psicológicos reales: Los estudios del Ministerio de Educación (2023) y la evidencia del archivo adjunto muestran que la violencia digital provoca:

ansiedad, depresión, aislamiento social, descenso académico, afectación prolongada a la salud mental.

Todo ello justifica la urgencia de proponer reformas legislativas, protocolos de aplicación y modelos comparados de tipificación, que es uno de los aportes prácticos que ofrecerá el artículo. Contrasta tipos penales existentes con categorías criminológicas modernas, lo que permite evaluar si el COIP cumple su función de protección eficaz frente a formas contemporáneas de violencia digital.

El caso colombiano resulta relevante como experiencia comparada, no por la existencia de un delito penal autónomo de ciberacoso —figura que no se encuentra tipificada en su Código Penal—, sino por el desarrollo de un marco normativo complementario que aborda la violencia digital desde los delitos informáticos (Ley 1273 de 2009) y desde un enfoque preventivo y administrativo en el ámbito educativo (Ley 1620 de 2013). No obstante, la ausencia de un tipo penal general de ciberacoso en Colombia permite evidenciar que incluso ordenamientos jurídicos con avances normativos en materia digital presentan vacíos en la tutela penal integral

del hostigamiento digital reiterado.

Importancia social

El ciberacoso constituye una problemática creciente entre niños, adolescentes y jóvenes ecuatorianos, cuyas vidas están profundamente integradas a internet y redes sociales.

El archivo adjunto reporta que: El ciberacoso es una de las formas más comunes de violencia escolar. Puede mantenerse 24/7 debido a la disponibilidad tecnológica.

Puede causar daños irreparables, especialmente cuando involucra humillación pública o ataques reiterados.

La ausencia de un tipo penal específico genera desprotección estructural, violando los derechos constitucionales de integridad y dignidad, así como compromisos internacionales de protección a la niñez y a los grupos vulnerables.

Por ello, el análisis crítico del COIP no solo responde a una inquietud académica, sino a una exigencia social urgente, contribuyendo al diseño de una política penal más coherente y eficaz.

El trabajo es importante porque:

- Llena un vacío teórico en la literatura jurídica penal ecuatoriano;
- Aporta una metodología integral para estudiar el ciberacoso en su dimensión constitucional, penal y social;
- Ofrece propuestas aplicadas para mejorar la legislación y la práctica judicial;
- Responde a una problemática social de alto impacto, documentada tanto en estudios oficiales como en investigaciones científicas;

La falta de un estudio integrador que examine el ciberacoso desde el derecho penal, el derecho constitucional y los estándares de protección de datos, tomando como

referencia experiencias comparadas como la colombiana. Coloca a Ecuador en diálogo con tendencias comparadas que ya reconocen el ciberacoso como delito autónomo.

OBJETIVOS

Examinar de manera crítica y sistemática la respuesta penal ecuatoriana frente al ciberacoso, mediante el análisis del Código Orgánico Integral Penal (COIP) y su relación con los derechos constitucionales de integridad, honra, intimidad y protección de datos personales, así como la revisión de doctrina, políticas públicas y experiencias comparadas —especialmente del modelo colombiano— con el fin de determinar las brechas normativas existentes y proponer lineamientos técnico–jurídicos que permitan mejorar la eficacia de la protección penal frente al hostigamiento digital.

OBJETIVO GENERAL

Analizar si la ausencia de un tipo penal autónomo de ciberacoso en el Código Orgánico Integral Penal genera un déficit de protección penal y dificultades de subsunción típica que afectan el principio de legalidad y el acceso a la justicia de las víctimas, mediante un estudio dogmático y comparado con modelos normativos extranjeros.

Este objetivo se sustenta en la evidencia doctrinaria y normativa previamente identificada:

- El COIP no tipifica directamente el ciberacoso, lo que obliga a subsumir estas conductas en tipos dispersos como el hostigamiento digital (COIP, art. 154.2), violencia psicológica (art. 157), violación a la intimidad (art. 178), difusión de información restringida (art. 180) o revelación ilegal de bases de datos (art. 229).

- Estudios científicos como los de Pozo Chugá (2025) señalan que esta fragmentación genera vacíos de protección, dificultades probatorias y respuestas penales insuficientes.
- Zúñiga Vásquez (2021) demuestra que la ausencia de un tipo penal propio vulnera el principio de taxatividad penal, pues el acoso digital se ajusta forzadamente a tipos tradicionales.
- El Consejo de Comunicación (2020) advierte que el ciberacoso se ha intensificado tras la pandemia y que el ordenamiento penal ecuatoriano "no está preparado para responder a la complejidad digital actual".
- El Ministerio de Educación (2023) reconoce que el ciberacoso tiene efectos psicológicos severos y puede transformarse en hostigamiento permanente, lo que exige un marco penal actualizado.
- La Constitución protege bienes jurídicos afectados directamente por el ciberacoso: integridad física y psíquica (art. 66.3), intimidad y honra (art. 66.8), protección de datos personales (art. 66.19).

Dado este panorama, un análisis crítico del COIP y del sistema penal ecuatoriano no solo es pertinente sino necesario, y el Objetivo General se alinea directamente con el problema de estudio: la ausencia de un marco penal integral frente al ciberacoso.

OBJETIVOS ESPECÍFICOS

Analizar si la ausencia de un tipo penal autónomo de ciberacoso en el Código Orgánico Integral Penal genera un déficit de protección penal y dificultades de subsunción típica que afectan el principio de legalidad y el acceso a la justicia de las víctimas, mediante un estudio dogmático y comparado con modelos normativos extranjeros.

- Examinar el concepto jurídico–penal de ciberacoso y sus elementos constitutivos desde la doctrina penal y los estándares de derechos fundamentales.
- Identificar y analizar las disposiciones del Código Orgánico Integral Penal aplicables a conductas de acoso digital, evaluando las dificultades de subsunción típica existentes.
- Analizar las implicaciones de la actual regulación penal del ciberacoso en relación con el principio de legalidad y el acceso a la justicia de las víctimas.
- Examinar la correspondencia entre el marco penal vigente y los derechos constitucionales afectados por el ciberacoso, en particular la integridad psíquica, la honra y la intimidad.
- Comparar el tratamiento jurídico del ciberacoso en el ordenamiento ecuatoriano con modelos normativos adoptados en otros países, a fin de identificar buenas prácticas legislativas.
- Proponer lineamientos de reforma normativa orientados a fortalecer la protección penal frente al ciberacoso en el Ecuador.

Derecho comparado

Comparar la regulación del ciberacoso en el ordenamiento jurídico ecuatoriano con modelos de tipificación penal o medidas de protección adoptadas en otros sistemas jurídicos, a fin de identificar buenas prácticas normativas.

El análisis comparado es viable porque sistemas como el colombiano ya cuentan con delimitaciones penales más claras frente al acoso digital (Consejo de Comunicación, 2020) y estudios como los de Pozo Chugá (2025) muestran la necesidad de adoptar estándares regionales.

Propuesta jurídica

Proponer lineamientos de interpretación o reforma normativa orientados a fortalecer la protección penal frente al ciberacoso, en armonía con el principio de legalidad y los estándares de derechos humanos.

Formular recomendaciones y lineamientos técnico–jurídicos orientados a la creación de un tipo penal autónomo de ciberacoso, o en su defecto, la modificación del COIP para cubrir las modalidades actuales del hostigamiento digital. La Ley Orgánica de Protección de Datos Personales (2021) establece principios clave sobre tratamiento indebido de información que también operan en contextos de acoso digital.

MARCO TEÓRICO

1. Conceptualización del ciberacoso.

El ciberacoso se define como una forma de acoso, hostigamiento o agresión continuada realizada mediante el uso de tecnologías digitales, tales como redes sociales, servicios de mensajería instantánea, correo electrónico y plataformas virtuales. Este fenómeno comprende conductas como la intimidación, la humillación, la difusión de contenido falso o íntimo sin autorización, las amenazas, la suplantación de identidad y la vigilancia permanente. Su carácter reiterado y su ejecución en entornos digitales incrementan la gravedad del daño causado a las víctimas.

La doctrina penal ecuatoriana y la literatura jurídica especializada coinciden en que el ciberacoso presenta características diferenciadoras respecto del acoso tradicional. Entre estos elementos se destacan el anonimato del agresor, la permanencia del contenido en entornos digitales, la velocidad y amplitud de su difusión, así como la posibilidad de reiteración indefinida de las conductas. Estas particularidades incrementan el impacto del daño psíquico y emocional en la víctima, y dificultan la prevención y persecución penal mediante categorías normativas concebidas para contextos analógicos. Estas características agravan el daño psicológico de las víctimas y dificultan mecanismos clásicos de prevención.

En el contexto de las sociedades contemporáneas, el ciberacoso se entiende no solo

como una manifestación de violencia individual, sino como un fenómeno social que afecta la dignidad, la integridad psicológica, la tranquilidad, la autoestima y la seguridad de las víctimas, y en particular tiene un impacto grave cuando las víctimas son grupos vulnerables como niñas, niños, adolescentes, mujeres o minorías.

2. Delimitación conceptual del objeto de estudio

El presente artículo adopta una **delimitación conceptual precisa** del fenómeno del ciberacoso, con el fin de evitar confusiones terminológicas y garantizar coherencia jurídica en el análisis penal.

A efectos de esta investigación, el **ciberacoso** se entiende como una **conducta de hostigamiento reiterado**, realizada mediante tecnologías de la información y comunicación, redes sociales o plataformas digitales, que tiene como finalidad o resultado **afectar la integridad psíquica** (CRE, 2008)**, emocional o la dignidad de la víctima**, con independencia de que exista o no una relación previa entre agresor y víctima. Esta definición abarca conductas como insultos persistentes, humillaciones públicas, amenazas no físicas, difusión reiterada de contenido perjudicial, creación de perfiles falsos con fines de hostigamiento y campañas sistemáticas de descrédito en entornos digitales.

Es importante diferenciar el **ciberacoso** de otras categorías jurídicas relacionadas, pero conceptualmente distintas. En primer lugar, el **cyberbullying** suele circunscribirse a contextos escolares o entre pares, especialmente cuando las víctimas son niñas, niños o adolescentes, y su tratamiento normativo en varios países se ha desarrollado principalmente desde enfoques educativos y preventivos. Si bien este fenómeno se menciona como antecedente relevante, el análisis del presente artículo **no se limita al ámbito escolar**, sino que aborda el ciberacoso como una conducta que puede afectar a cualquier persona.

En segundo lugar, el **ciberhostigamiento o stalking digital** implica un patrón de persecución, vigilancia o acecho continuo (digital A. , 2023), que en algunos ordenamientos

jurídicos cuenta con tipificaciones específicas. Aunque comparte elementos con el ciberacoso, como la reiteración y el uso de medios digitales, el stalking suele requerir una relación más directa de seguimiento individualizado, por lo que se lo considera una categoría diferenciada.

El ciberacoso se caracteriza por la reiteración y la permanencia del daño, el art. 154.2 no desarrolla claramente la reiteración, sino que se centra en la finalidad del daño

Asimismo, este estudio **no tiene como objeto central la violencia sexual digital** (Barreto CAlderón, 2024), entendida como la difusión no consentida de contenido íntimo, el grooming, la pornografía infantil digital o el contacto sexual mediante medios electrónicos. Estas conductas ya han sido parcialmente incorporadas en el ordenamiento penal ecuatoriano a través de reformas recientes al Código Orgánico Integral Penal y responden a una lógica de protección penal específica de la libertad e integridad sexual.

En consecuencia, cuando en el texto se mencionan fenómenos como la denominada "pornografía de venganza", la difusión maliciosa de datos personales o determinadas formas de persecución digital, ello se realiza **únicamente con fines ilustrativos o contextuales**, para evidenciar la complejidad del entorno digital y los límites del marco penal vigente, mas no como parte del núcleo del análisis.

De este modo, el objeto central de la investigación se delimita al **ciberacoso no necesariamente sexual** (Zúñiga Vásquez, 2021), caracterizado por el hostigamiento digital reiterado y el daño psíquico prolongado, y a su **insuficiente encaje en los tipos penales actualmente previstos en el COIP** (Pozo Chugá, 2025), lo cual genera vacíos normativos, inseguridad jurídica y dificultades en la protección efectiva de las víctimas.

3. Impacto humano y social del ciberacoso.

Desde un enfoque humanístico, el ciberacoso no es únicamente un problema tecnológico o penal, sino una forma de violencia que vulnera la dignidad humana y la integridad emocional. Señala que las víctimas experimentan ansiedad, depresión, aislamiento, miedo y

daños en su autoestima, especialmente cuando se trata de menores o mujeres expuestas a violencia sexual digital.

La violencia digital también reproduce desigualdades estructurales y patrones de discriminación, lo que convierte su regulación en una obligación ética y jurídica del Estado.

4. Situación jurídica en Ecuador.

Aunque el COIP regula delitos como amenazas, hostigamiento, violación a la intimidad, divulgación de información reservada o violencia psicológica, ninguno aborda explícitamente el ciberacoso como delito autónomo. Las investigaciones de (Barreto, 2024) coinciden en que la falta de tipificación viola el principio de legalidad y deja desprotegidas a las víctimas.

La inexistencia de una tipificación penal autónoma genera obstáculos relevantes en la obtención y conservación de pruebas digitales, en la identificación efectiva de los responsables y en la aplicación oportuna de mecanismos de protección para las personas afectadas.

El fenómeno del ciberacoso se ha consolidado como una problemática de creciente incidencia en Ecuador, evidenciando retos sustanciales derivados de la insuficiencia normativa y de la necesidad de adecuar el ordenamiento jurídico a las dinámicas propias del entorno digital. Esta forma de violencia impacta a personas de distintos grupos etarios y, ante la carencia de un marco legal sólido, se ve limitada tanto la tutela efectiva de las víctimas como la sanción de las conductas ilícitas. En contraste, el sistema jurídico español incorpora disposiciones específicas que configuran un esquema normativo más desarrollado para la prevención, investigación y sanción del ciberacoso. En este contexto, la presente investigación tiene como finalidad efectuar un estudio comparado entre la regulación jurídica del ciberacoso en Ecuador y España, con el propósito de identificar puntos de convergencia, divergencias y oportunidades de mejora. Para ello, se emplea una metodología de carácter cualitativo, basada en el análisis documental de normas legales vigentes, doctrina especializada y resoluciones

judiciales relevantes. Como resultado, se elaborará un informe analítico que formule propuestas orientadas al fortalecimiento del marco normativo ecuatoriano, tomando como referencia las experiencias legislativas españolas y otros estándares internacionales, a fin de enfrentar de manera más eficaz el ciberacoso en el entorno digital (Barreto, 2024).

5. Estado normativo en Ecuador: el COIP y su tratamiento (o ausencia) del ciberacoso.

- En Ecuador, el Código Orgánico Integral Penal (COIP) — vigente desde 2014 — representó un avance: sustituyó leyes anteriores, sistematizó delitos y agregó nuevas figuras penales. (Penal C. O., 2014)
- En algunos casos de violencia digital o acoso mediante TIC, pueden aplicarse disposiciones existentes (amenazas, injurias, calumnias, violencia psicológica, delitos contra la intimidad, abuso sexual digital si media material sexual, etc.). (Pozo, 01/05/2025)
- Diversos trabajos académicos han propuesto reformas normativas: establecer un tipo penal autónomo para ciberacoso / cyberbullying, con definición clara, elementos típicos definidos (conducta, medios digitales, daño emocional/psicológico, repetición, etc.), para garantizar el principio de legalidad y los derechos de las víctimas. (Alexandra, JULIO-2021)

6. Vacíos normativos, retos para la persecución penal y propuestas: hacia una respuesta integral.

- En consecuencia, de la falta de tipificación clara, existe una "inseguridad jurídica": víctimas de ciberacoso pueden quedar desprotegidas, sin acceso efectivo a justicia, con dificultad para denunciar, recabar evidencias, o lograr sanciones. Esto atenta contra su derecho a la reparación, a la protección, a la justicia.
- Las dificultades probatorias — especialmente con evidencia digital (mensajes, capturas de pantalla, logs, metadata, anonimato, borrado, cifrado) — La doctrina penal ecuatoriana ha advertido que las dificultades probatorias propias del entorno digital —como la

preservación de mensajes, capturas de pantalla, registros electrónicos, metadatos y la identificación del autor bajo condiciones de anonimato— exigen no solo reformas normativas, sino también capacitación institucional, protocolos especializados de recolección y preservación de evidencia digital, así como mecanismos de cooperación interinstitucional e internacional, dada la naturaleza transnacional del ciberespacio.

- Desde la doctrina penal contemporánea se ha propuesto que la normativa penal incorpore un tipo autónomo de ciberacoso o cyberbullying, con una definición clara de sus elementos típicos, sanciones proporcionales y medidas de protección específicas para las víctimas. Estas propuestas parten del reconocimiento de que el hostigamiento digital reiterado produce daños psíquicos reales y continuados que no siempre encuentran una adecuada subsunción en los tipos penales tradicionales.

Derecho comparado: aproximaciones normativas al ciberacoso y la violencia digital

El análisis del derecho comparado permite identificar distintas estrategias normativas adoptadas por los Estados para enfrentar el fenómeno del ciberacoso y otras formas de violencia digital. Estas estrategias no son uniformes y varían entre modelos de **tipificación penal directa**, **regulación sectorial**, **agravantes digitales** y **enfoques preventivos o administrativos**. A continuación, se examinan los principales referentes regionales y europeos relevantes para el caso ecuatoriano.

España

España ha desarrollado uno de los modelos más avanzados en materia de protección frente al acoso, aunque **no utiliza expresamente el término "ciberacoso" como tipo autónomo**. El Código Penal español tipifica el delito de **acoso o stalking** (art. 172 ter), permitiendo expresamente que la conducta se cometa **mediante tecnologías de la información y comunicación**.

Este modelo se caracteriza por:

- la persecución reiterada,
- la alteración grave de la vida cotidiana de la víctima,
- el reconocimiento explícito del uso de medios digitales como agravante o medio comisivo.

Asimismo, el ordenamiento español sanciona de manera específica la **difusión no consentida de imágenes íntimas**, lo que evidencia un enfoque penal que incorpora la dimensión tecnológica como factor de agravación. España adopta, por tanto, un **modelo penal híbrido**, donde el acoso general se adapta al entorno digital sin crear un tipo autónomo de "ciberacoso".

México

México ha optado por un enfoque diferenciado a través de la denominada **Ley Olimpia**, que no constituye un único cuerpo legal, sino un conjunto de reformas a los códigos penales federal y estatales. Este modelo se centra principalmente en la **violencia digital**, en especial la difusión no consentida de contenido íntimo, el hostigamiento digital y las amenazas en línea, con un marcado **enfoque de género**.

Si bien la legislación mexicana no tipifica un delito general de ciberacoso aplicable a toda la población, sí establece:

- tipos penales específicos de violencia digital,
- agravantes por difusión masiva,
- mecanismos de remoción de contenido.

Este enfoque resulta relevante como **modelo de protección reforzada**, aunque su alcance se encuentra focalizado en determinadas manifestaciones del daño digital.

Colombia

Colombia **no cuenta con un delito penal autónomo de ciberacoso** en su Código

Penal. No obstante, ha desarrollado un marco normativo complementario que aborda el fenómeno desde distintos ángulos.

Por un lado, la **Ley 1273 de 2009** incorporó los **delitos informáticos**, orientados a la protección de datos, sistemas y información, pero **no regula el hostigamiento digital reiterado como forma de violencia psíquica**.

Por otro lado, la **Ley 1620 de 2013** creó el Sistema Nacional de Convivencia Escolar, reconociendo expresamente el **ciberacoso escolar** como una forma de violencia, aunque desde un enfoque **preventivo, administrativo y educativo**, no penal.

El modelo colombiano resulta ilustrativo porque evidencia que, aun con avances en materia digital y educativa, **persiste la ausencia de un tipo penal general de ciberacoso**, lo que refuerza la tesis de que la fragmentación normativa no garantiza una tutela penal integral del hostigamiento digital.

Chile

Chile ha avanzado progresivamente en la regulación de la violencia digital. La **Ley 21.153** penaliza la difusión no consentida de imágenes íntimas, y existen reformas y proyectos orientados a sancionar la suplantación de identidad digital, el hostigamiento y otras formas de acoso en línea.

Aunque no existe aún un delito autónomo de ciberacoso de alcance general, el modelo chileno se caracteriza por:

- la incorporación de tipos penales específicos vinculados al entorno digital,
- el reconocimiento del daño moral y psíquico,
- la tendencia hacia una regulación integral de la violencia digital.

El análisis comparado demuestra que, incluso en ordenamientos jurídicos con avances significativos en materia de violencia digital, como España, México, Colombia y Chile, no existe un consenso uniforme en torno a la tipificación penal autónoma del ciberacoso. Sin

embargo, estos modelos coinciden en reconocer la insuficiencia de las figuras penales tradicionales para abordar el hostigamiento digital reiterado, lo que refuerza la necesidad de una respuesta penal específica y sistemática. En el caso ecuatoriano, la ausencia de un tipo penal autónomo evidencia un déficit normativo que justifica la propuesta de reforma planteada en el presente artículo.

Análisis crítico del COIP y sus brechas normativas.

El COIP presenta varias falencias frente al ciberacoso:

- **Ausencia de tipificación clara**

No existe un delito autónomo de ciberacoso, lo cual afecta el principio de legalidad penal y dificulta la judicialización de casos.

- **Falta de enfoque de derechos humanos**

No se reconoce la violencia digital como una amenaza a la dignidad, integridad emocional e intimidad, especialmente para mujeres, niñas, niños y adolescentes.

- **Problemas probatorios**

La normativa no regula explícitamente la preservación de evidencia digital, cadena de custodia electrónica ni técnicas de investigación cibernética.

- **Respuesta institucional insuficiente**

Las víctimas carecen de mecanismos de denuncia en línea, medidas de protección inmediata o acompañamiento psicológico especializado.

- **Desactualización frente a estándares internacionales**

Ecuador no ha incorporado las mejores prácticas de España, México o Chile, donde se legisla la violencia digital de manera integral.

MARCO METODÓLOGICO

Diseño metodológico

La presente investigación adopta un **enfoque cualitativo**, de tipo **documental–analítico**, propio de los estudios jurídicos orientados al examen crítico de normas, principios constitucionales, doctrina especializada y derecho comparado.

El estudio se sustenta exclusivamente en el **análisis de fuentes documentales**, sin incorporar técnicas de recolección de datos empíricos como, dado que el objetivo central es **evaluar la coherencia, suficiencia y eficacia del marco normativo penal ecuatoriano frente al ciberacoso**, y no medir percepciones sociales o estadísticas de incidencia.

Conducta Típica

El **ciberacoso típico**, tal como se manifiesta en la realidad social y digital, **no siempre tiene finalidad física ni sexual**, sino que produce:

- daño psíquico,
- humillación pública,
- control emocional,
- intimidación sostenida,
- afectación a la dignidad y tranquilidad personal

Tipo de investigación

La investigación es:

- **Cualitativa**, porque analiza contenidos normativos, doctrinales y jurídicos desde una perspectiva interpretativa.
- **Documental**, porque se basa en fuentes primarias y secundarias de carácter

jurídico.

- **Analítica y crítica**, porque examina las disposiciones del Código Orgánico Integral Penal (COIP) a la luz de los derechos constitucionales y de modelos comparados.

Técnicas de recolección de información

Se emplearon las siguientes técnicas:

1. **Revisión normativa**

- Constitución de la República del Ecuador (2008).
- Código Orgánico Integral Penal (COIP).
- Ley Orgánica de Protección de Datos Personales.
- Proyectos de ley y normativa conexa sobre violencia digital.

2. **Revisión doctrinal**

- Artículos científicos, tesis y estudios académicos ecuatorianos sobre ciberacoso, violencia digital y principio de legalidad penal.

3. **Derecho comparado**

- Análisis de modelos normativos de España, México, Colombia y Chile, con énfasis en la existencia o ausencia de tipos penales autónomos de ciberacoso.

Técnica de análisis

El análisis se realizó mediante:

- **Interpretación sistemática** de normas penales y constitucionales.
- **Análisis crítico** de vacíos normativos y dispersión legislativa.
- **Contraste normativo** entre el COIP y los derechos constitucionales vulnerados por el ciberacoso.
- **Comparación jurídica** con ordenamientos extranjeros relevantes.

Delimitación metodológica

El estudio **no incluye trabajo de campo**, entrevistas, encuestas ni análisis estadístico, ya que ello excede el alcance de un artículo científico jurídico–dogmático. No obstante, se reconoce que futuras investigaciones podrían complementar este análisis mediante estudios empíricos que evalúen la percepción social o la aplicación práctica del marco normativo vigente.

ANÁLISIS DE RESULTADOS

El análisis documental y normativo realizado permite identificar una serie de **resultados jurídicos relevantes** en relación con la respuesta penal ecuatoriana frente al ciberacoso, particularmente en lo que respecta al Código Orgánico Integral Penal (COIP) y su armonización con el marco constitucional.

1. Confirmación de la ausencia de un tipo penal autónomo de ciberacoso

Como primer resultado, se constata que el **ordenamiento penal ecuatoriano no contempla un tipo penal autónomo de ciberacoso**. El COIP regula conductas vinculadas al uso de tecnologías de la información de manera **dispersa**, a través de figuras como el hostigamiento por medios tecnológicos, la violencia psicológica, la violación a la intimidad, la difusión de información restringida y determinados delitos sexuales cometidos mediante medios electrónicos.

Este hallazgo confirma el problema de investigación planteado, en tanto **ninguna de estas figuras penales aborda de manera integral el hostigamiento digital reiterado con daño psíquico**, característica central del ciberacoso no necesariamente sexual.

2. Verificación de la fragmentación normativa en el COIP

El artículo 154.2 del Código Orgánico Integral Penal, introducido mediante la reforma de 2021 sobre violencia sexual digital, tiene como bien jurídico protegido la **integridad personal de la víctima**, comprendida en sus dimensiones **física, psíquica, emocional y de dignidad**. No obstante, el diseño normativo del tipo revela que la tutela penal se encuentra condicionada a una **finalidad específica de daño**, lo cual restringe de manera significativa su ámbito de aplicación frente a conductas de hostigamiento digital reiterado.

Desde una perspectiva constitucional, el bien jurídico de la **integridad psíquica** goza de protección autónoma; sin embargo, el tipo penal no desarrolla una protección suficiente de este bien cuando el daño no es consecuencia directa de una agresión física o sexual, sino de un proceso de hostigamiento digital continuado.

2.1. Elementos objetivos del tipo penal

El elemento objetivo del artículo 154.2 COIP exige la concurrencia de los siguientes componentes:

a) **Una conducta de hostigamiento**,

b) **Realizada a través de medios tecnológicos o digitales**,

c) **Que implique búsqueda de cercanía con la víctima**,

d) **Dirigida a causar daño a la integridad física, psíquica, emocional o a la dignidad personal**.

Este diseño típico presenta una limitación estructural relevante: la exigencia de una *búsqueda de cercanía* y de una *finalidad específica de daño* no siempre se manifiestan en las conductas de ciberacoso tal como se presentan en la realidad social y digital. En numerosos casos, el hostigamiento digital se expresa mediante humillaciones públicas, campañas de descrédito, creación de perfiles falsos o ataques masivos, sin que exista una relación directa de cercanía ni una intención explícita de causar daño físico o sexual.

2.2. Elemento subjetivo del tipo penal

Desde el punto de vista subjetivo, el artículo 154.2 COIP exige **dolo directo**, esto es, la voluntad consciente de hostigar con la finalidad de causar un daño determinado a la integridad de la víctima. Esta exigencia excluye supuestos frecuentes de ciberacoso en los que el daño psíquico se produce como **resultado objetivo del hostigamiento reiterado**, aun cuando el agresor alegue ausencia de intención directa o se ampare en supuestas conductas de "broma", "opinión" o "libertad de expresión".

La configuración del tipo penal, por tanto, no admite adecuadamente el **dolo eventual**, ni contempla el daño psíquico como resultado suficiente del comportamiento, lo que genera escenarios de atipicidad material.

2.3. Falta de encaje del ciberacoso típico en el art. 154.2 COIP

El ciberacoso, entendido como hostigamiento digital reiterado que produce humillación pública, intimidación sostenida, control emocional o afectación prolongada a la tranquilidad personal, **no siempre persigue un daño físico ni sexual**, ni se manifiesta mediante una relación directa de cercanía entre agresor y víctima.

En consecuencia, múltiples conductas de ciberacoso no encajan adecuadamente en el artículo 154.2 COIP, lo que obliga a una subsunción forzada o conduce al archivo de denuncias por atipicidad. Esta situación evidencia que el tipo penal fue diseñado con un enfoque restringido, vinculado principalmente a la violencia sexual digital, y no al fenómeno amplio del hostigamiento digital reiterado.

2.4. Ejemplos de subsunción fallida

A modo ilustrativo, pueden señalarse los siguientes supuestos problemáticos:

- humillaciones públicas reiteradas en redes sociales sin contacto directo con la víctima;
- creación de perfiles falsos para ridiculizar o acosar;

- campañas digitales de descrédito sin amenaza física;
- control emocional digital mediante mensajes constantes no sexuales.

En estos casos, el daño psíquico es real y verificable, pero **no se configura la finalidad típica exigida por el artículo 154.2**, lo que impide una respuesta penal eficaz.

2.5. Jurisprudencia y criterio de atipicidad

La práctica judicial evidencia que, ante la ausencia de un tipo penal autónomo de ciberacoso, los operadores de justicia recurren a figuras penales colaterales o archivan los procesos por falta de adecuación típica. Este fenómeno ha sido advertido por la doctrina penal ecuatoriana, que señala que la aplicación extensiva del artículo 154.2 COIP vulnera el principio de legalidad y taxatividad penal, al pretender abarcar conductas para las cuales el tipo no fue diseñado.

3. Dificultades de subsunción típica y consecuencias procesales

Un resultado central del análisis es la **existencia de dificultades reales de subsunción típica** en casos de ciberacoso. Conductas como la humillación pública reiterada en redes sociales, la creación de perfiles falsos para hostigar, el control emocional digital o las campañas de descrédito en línea **no encajan plenamente en los tipos penales vigentes**.

Esta situación genera consecuencias procesales concretas, tales como:

- archivo de denuncias por atipicidad,
- recalificaciones forzadas a tipos penales no diseñados para el entorno digital,
- respuestas penales parciales e insuficientes.

Lo anterior afecta directamente el **principio de legalidad y taxatividad penal**, al obligar a operadores de justicia a forzar la interpretación de tipos tradicionales para abarcar fenómenos digitales complejos.

"A fin de evidenciar de manera sistemática las dificultades de subsunción típica que presenta el ordenamiento penal ecuatoriano frente a las conductas de ciberacoso, se incorpora

la siguiente matriz de subsunción típica, en la cual se contrastan conductas digitales frecuentes con los tipos penales actualmente previstos en el Código Orgánico Integral Penal, permitiendo identificar de forma clara los vacíos normativos y las fallas de encaje dogmático."

Tabla X. Matriz de subsunción típica de conductas de ciberacoso en el COIP

Conducta digital reiterada	**Tipo penal COIP aplicable**	**¿Existe encaje típico?**	**Razón del fallo de subsunción**
Humillación reiterada en redes sociales (comentarios, memes, etiquetas ofensivas)	Art. 154.2 COIP (hostigamiento por medios tecnológicos)	✗ Parcial	El tipo exige finalidad de daño físico, psíquico o sexual; la humillación pública reiterada no siempre persigue dicha finalidad
Conducta digital reiterada	**Tipo penal COIP aplicable**	**¿Existe encaje típico?**	**Razón del fallo de subsunción**
Creación de perfiles falsos para hostigar o ridiculizar	Art. 154.2 COIP	✗ No	No se configura "búsqueda de cercanía" ni daño físico o sexual
Campañas digitales de descrédito o burla sistemática	Art. 182 COIP (injurias/calumnia)	✗ Insuficiente	Requiere imputación concreta; no abarca hostigamiento reiterado ni daño psíquico continuado
Amenazas no físicas reiteradas por mensajería o redes	Art. 154 COIP (amenazas)	✗ Parcial	El tipo se orienta a amenazas graves; no cubre intimidación psicológica sostenida
Control emocional digital (mensajes constantes, presión psicológica)	Art. 157 COIP (violencia psicológica)	✗ No	Se limita a relaciones familiares o de género
Difusión reiterada de contenido no íntimo pero perjudicial	Arts. 178–180 COIP (intimidad/datos)	✗ No	Protegen información íntima o reservada, no daño psíquico ni hostigamiento
Hostigamiento digital sin finalidad sexual	Art. 173–174 COIP	✗ No	Tipos exclusivamente sexuales
Vigilancia digital abusiva (seguimiento en línea constante)	Ninguno específico	✗ No	Vacío normativo absoluto

Tabla x: Elaboración propia a partir del COIP y la Const. de la República del Ecuador.

"La matriz precedente demuestra que el ciberacoso, en su manifestación no necesariamente sexual, no logra una subsunción típica adecuada en el COIP, obligando a una aplicación fragmentada y forzada de tipos penales diseñados para contextos distintos. Esta situación vulnera el principio de legalidad y taxatividad penal, al no permitir a las víctimas ni a los operadores de justicia identificar con claridad la conducta prohibida y su consecuencia jurídica, confirmando la existencia de un vacío normativo estructural."

4. Déficit de protección de la integridad psíquica frente al ciberacoso

El análisis revela que, si bien la Constitución de la República del Ecuador reconoce la **integridad psíquica, la honra y la dignidad** como derechos fundamentales, el COIP **no desarrolla una protección penal específica y adecuada de estos bienes jurídicos en el contexto digital**.

El artículo 157 del COIP, referido a la violencia psicológica, se limita a ámbitos específicos como relaciones familiares o violencia contra la mujer, lo que excluye múltiples escenarios de ciberacoso que se producen fuera de dichas relaciones. Este resultado confirma un **déficit de protección penal** frente a una forma de violencia que se manifiesta de manera transversal en el entorno digital.

5. Desarmonización entre el marco constitucional y el marco penal

Otro resultado relevante es la **desarmonización entre el marco constitucional y el marco penal**. Mientras la Constitución garantiza de manera amplia la integridad psíquica, la intimidad, la honra y la protección de datos personales, el COIP ofrece una respuesta fragmentada que **no asegura una tutela penal efectiva frente al ciberacoso**.

Esta falta de correspondencia normativa afecta el **acceso a la justicia de las víctimas**, quienes enfrentan barreras jurídicas para la judicialización de hechos que, aunque lesivos y reiterados, no se adecuan plenamente a los tipos penales existentes.

6. Confirmación de la necesidad de una reforma penal específica

Finalmente, el análisis de resultados permite confirmar que la **ausencia de un tipo penal autónomo de ciberacoso genera un vacío normativo relevante** en el sistema penal ecuatoriano. Este vacío no solo limita la capacidad del Estado para sancionar conductas de hostigamiento digital, sino que también debilita la función preventiva y protectora del derecho penal.

Los resultados obtenidos respaldan la necesidad de **incorporar una figura penal**

específica o un marco normativo integral que contemple el ciberacoso no sexual, caracterizado por el hostigamiento reiterado y el daño psíquico, de conformidad con los principios constitucionales y las exigencias del entorno digital contemporáneo.

DISCUSIÓN

La discusión de los resultados obtenidos permite profundizar en el **alcance real del problema jurídico identificado**, así como en las **implicaciones dogmáticas, constitucionales y procesales** que genera la ausencia de un tipo penal autónomo de ciberacoso en el ordenamiento jurídico ecuatoriano. A partir del análisis normativo desarrollado, se evidencia que el tratamiento penal actual del ciberacoso no responde de manera adecuada a la complejidad del fenómeno digital contemporáneo.

En primer lugar, los resultados confirman que el **Código Orgánico Integral Penal (COIP)** regula conductas relacionadas con el uso indebido de tecnologías de la información de forma **fragmentada y sectorial**, lo que impide una protección penal integral frente al ciberacoso. La dispersión normativa observada en los artículos 154.2, 157, 178, 180 y 229 del COIP revela que el legislador ha optado por **respuestas parciales**, orientadas a bienes jurídicos específicos, sin desarrollar una figura penal que abarque el **hostigamiento digital reiterado como fenómeno autónomo**.

Desde una perspectiva dogmática, esta fragmentación se traduce en **problemas estructurales de tipicidad**. El análisis del artículo 154.2 COIP resulta ilustrativo, pues si bien reconoce el hostigamiento por medios tecnológicos, **condiciona la punibilidad a la finalidad de causar** daño a la integridad física, psíquica, emocional o dignidad persona **de la víctima**. Esta exigencia típica excluye un amplio espectro de conductas de ciberacoso que producen **daño psíquico, emocional y social**, pero que no persiguen una agresión física ni sexual. En consecuencia, el tipo penal no logra captar la esencia del ciberacoso no sexual, caracterizado

por la reiteración, el control emocional, la humillación pública y la afectación prolongada a la tranquilidad personal.

Esta limitación normativa adquiere mayor relevancia si se considera que el **bien jurídico principalmente afectado por el ciberacoso es la integridad psíquica**, junto con la dignidad y la honra de la persona. La Constitución de la República del Ecuador reconoce expresamente estos derechos como bienes jurídicos fundamentales, lo que genera una **exigencia de coherencia** entre el marco constitucional y el derecho penal. Sin embargo, los resultados del análisis muestran que el COIP **no desarrolla una tutela penal específica de la integridad psíquica en el entorno digital**, lo que evidencia una brecha entre la protección constitucional y la respuesta penal efectiva.

Asimismo, el artículo 157 COIP, relativo a la violencia psicológica, no logra subsanar este vacío, ya que su ámbito de aplicación se encuentra restringido a **relaciones familiares o contextos de violencia contra la mujer**. Esta delimitación excluye múltiples escenarios de ciberacoso que se producen entre personas sin relación previa, en espacios abiertos como redes sociales, foros o plataformas digitales. En estos casos, pese a existir daño psicológico comprobable, el marco penal **no ofrece una vía clara de protección**, lo que refuerza la percepción de insuficiencia normativa.

Desde el punto de vista del **principio de legalidad y taxatividad penal**, la fragmentación normativa identificada genera efectos problemáticos. La ausencia de un tipo penal autónomo obliga a fiscales y jueces a realizar **interpretaciones extensivas o recalificaciones forzadas**, lo cual contradice los principios básicos del derecho penal moderno. En otros casos, la falta de adecuación típica conduce al **archivo de denuncias por atipicidad**, aun cuando los hechos denunciados evidencian un daño real y reiterado. Esta situación afecta directamente el **acceso a la justicia de las víctimas**, quienes se enfrentan a un sistema penal incapaz de responder de manera coherente a la violencia digital.

Desde una perspectiva procesal, los resultados permiten advertir que la dispersión de tipos penales genera **inseguridad jurídica**, tanto para las víctimas como para los operadores de justicia. La inexistencia de un tipo penal claro dificulta la identificación de los elementos probatorios relevantes, la valoración de la reiteración de la conducta y la adopción de medidas de protección oportunas. En el contexto digital, donde el daño puede amplificarse y prolongarse en el tiempo, esta carencia normativa resulta especialmente grave.

La discusión también pone de relieve que el problema del ciberacoso en Ecuador **no se limita a la ausencia de sanción penal**, sino que responde a una **falta de conceptualización legislativa del fenómeno digital**. El ciberacoso presenta características propias —anonimato, permanencia del contenido, difusión masiva, reiteración ilimitada— que no se corresponden plenamente con los supuestos tradicionales previstos en el COIP. La aplicación de tipos penales diseñados para contextos analógicos resulta insuficiente para capturar la complejidad de estas conductas.

En este sentido, el contraste con el derecho comparado permite observar que otros ordenamientos han avanzado hacia **tipificaciones específicas o mecanismos normativos más claros**, reconociendo el ciberacoso como una forma autónoma de violencia digital. No obstante, más allá de la experiencia comparada, los resultados obtenidos en este estudio demuestran que **el propio marco constitucional ecuatoriano justifica una revisión legislativa**, orientada a garantizar una protección penal efectiva de la integridad psíquica y la dignidad humana en el entorno digital.

Finalmente, la discusión reafirma que la ausencia de un tipo penal autónomo de ciberacoso **debilita la función preventiva y protectora del derecho penal**, al no ofrecer una respuesta clara frente a conductas que generan daños reales y prolongados. Esta debilidad normativa no solo afecta a las víctimas individuales, sino que también compromete la capacidad del Estado para enfrentar una forma de violencia que se ha intensificado con el uso

masivo de tecnologías digitales.

En consecuencia, los resultados discutidos permiten sostener que el ciberacoso constituye un **vacío normativo relevante en el sistema penal ecuatoriano**, cuya superación requiere una respuesta legislativa coherente con los principios constitucionales, el principio de legalidad y las exigencias del entorno digital contemporáneo. Esta discusión sienta las bases para formular propuestas normativas orientadas a fortalecer la tutela penal frente al ciberacoso y garantizar un acceso efectivo a la justicia para las víctimas.

PROPUESTA

I. Propuesta normativa concreta de reforma al COIP

1. Fundamento constitucional y normativa previa (síntesis)

La presente propuesta se fundamenta en la obligación constitucional del Estado ecuatoriano de garantizar la protección efectiva de la integridad psíquica, la dignidad, la honra, la intimidad y los datos personales, derechos reconocidos en los artículos 66 numerales 3, 8 y 19 de la Constitución de la República del Ecuador. Estos bienes jurídicos resultan directamente afectados por el ciberacoso, entendido como una forma de hostigamiento digital reiterado que produce daño psicológico prolongado y vulnera la tranquilidad personal de las víctimas.

Si bien el Código Orgánico Integral Penal regula diversas conductas vinculadas al uso indebido de tecnologías de la información, su tratamiento fragmentado impide una tutela penal integral del ciberacoso no necesariamente sexual. En este contexto, se justifica la incorporación de una figura penal autónoma que permita una respuesta coherente, proporcional y acorde con el principio de legalidad, evitando interpretaciones extensivas o subsunciones forzadas de tipos penales concebidos para contextos analógicos.

2. Texto sugerido para incorporación al COIP — Art. X. Ciberacoso

Propuesta de redacción (sugerida):

Art. X. — Ciberacoso.

Será sancionado con pena privativa de libertad de seis meses a tres años quien, **con dolo directo o eventual**, mediante el uso de tecnologías de la información, redes sociales o plataformas digitales, de manera reiterada y dirigida, realice actos de hostigamiento digital con capacidad real de causar afectación psíquica, emocional o menoscabo a la dignidad de una persona.

Se entenderá comprendido dentro del tipo penal el hostigamiento digital realizado mediante campañas sistemáticas o coordinadas, el uso de cuentas automatizadas o bots, la manipulación de imágenes, audios o videos mediante técnicas de inteligencia artificial o deepfakes, así como cualquier otra estrategia digital destinada a amplificar, reiterar o perpetuar el daño psíquico o la humillación pública de la víctima.

1 Agravantes (pena aumentada en un tercio):

- si la víctima es menor, mujer, adulto mayor o persona con discapacidad;
- si la difusión es masiva o viral;
- si se usan bots, perfiles automatizados o deepfakes;
- si se divulgan datos personales sensibles (doxxing).

2 Atenuantes especiales:

- reparación integral voluntaria previa al juicio;
- medidas restaurativas supervisadas cuando la víctima es menor y el daño no es grave.

3 Incorporar un artículo sobre MEDIDAS CAUTELARES DIGITALES

Esto coloca al paper en un nivel superior porque ningún país de la región lo regula bien.

Art. Y.- Medidas de protección y cautelares en casos de ciberacoso.

En los procesos por ciberacoso, el juez o jueza podrá disponer, de manera motivada y proporcional, una o varias de las siguientes medidas:

a) **Preservación forense digital inmediata**, ordenando a las plataformas, proveedores de servicios de internet o administradores de sistemas la conservación de registros, metadatos, direcciones IP, contenidos y demás evidencia digital relevante;

b) **Retiro, bloqueo o desindexación urgente de contenido digital** que constituya hostigamiento, humillación o daño psíquico, mediante orden judicial dirigida a las plataformas correspondientes;

c) **Prohibición de contacto digital**, directa o indirecta, entre el agresor y la víctima, incluyendo redes sociales, mensajería, correos electrónicos o cualquier medio tecnológico;

d) **Aseguramiento de la cadena de custodia electrónica**, garantizando la integridad, autenticidad y trazabilidad de la evidencia digital recolectada, conforme a protocolos técnicos especializados;

e) **Advertencia judicial a plataformas digitales** para impedir la creación de nuevas cuentas destinadas a la reiteración del hostigamiento, cuando existan indicios fundados de riesgo de repetición.

3. Justificación dogmática y constitucional de la propuesta

1. **Bien jurídico protegido.** La propuesta articula la protección penal de la **integridad psíquica, la dignidad y la honra**, bienes garantizados por la Constitución (art. 66) que actualmente carecen de una tutela penal integral en el entorno digital. Esto evita depender exclusivamente de figuras pensadas para contextos físicos.

2. **Elementos del tipo.** El texto distingue elementos objetivos (conducta, medio, reiteración) y subjetivos (dolo o, cuando proceda, dolo eventual). La reiteración se define mínimamente (dos acciones o más) para facilitar la subsunción sin dejar de garantizar la

taxatividad.

3. **Finalidad/resultado.** En lugar de condicionar la punibilidad a daño físico o sexual (limitan el art. 154.2 COIP), la propuesta permite sancionar cuando exista **resultado de daño psíquico o finalidad persecutoria**, corrigiendo la falla dogmática identificada en tu análisis. (Ver análisis art. 154.2 COIP en el documento).

4. **Proporcionalidad punitiva.** La horquilla penal propuesta (6 meses-3 años) busca ser **proporcional** a la gravedad del daño no físico, comparable con sanciones por hostigamiento y delitos contra la integridad moral en ordenamientos de la región, y permite la pena alternativa de multa en casos de menor entidad.

5. **Agravantes y protección de menores/vulnerables.** Concuerda con la línea protectora constitucional y con medidas reforzadas en normativa comparada (p. ej. agravantes por afectación de menores o difusión masiva como en algunos modelos latinoamericanos). Ejemplos: Ley Olimpia en México enfatiza agravantes cuando la víctima es menor o cuando la difusión es masiva.

4. Medidas procesales y de implementación (operativas)

1. **Órdenes de protección digital urgentes.** Crear procedimiento ágil (medidas cautelares provisionales) que permita la **suspensión temporal de cuentas** o remoción urgente de contenido cuando exista riesgo inminente de daño, mediante decisión judicial motivada.

2. **Preservación digital y custodia de evidencias.** Instruir mecanismos de **preservación de logs, metadatos y copia forense** a pedido judicial y con colaboración de proveedores de servicios —con controles para proteger datos personales— (armonizar con Ley Orgánica de Protección de Datos Personales).

3. **Cooperación con plataformas.** Establecer protocolos de **colaboración público- privada** que faciliten la identificación del autor y la retirada de contenidos ilícitos, con salvaguardas procesales (órdenes judiciales, plazos y control de proporcionalidad).

Modelos comparados muestran prácticas de requerimientos judiciales a plataformas (España, Chile, México).

4. **Formación y protocolos institucionales.** Capacitar a fiscales, jueces y policías en investigación digital (cadena de custodia electrónica, valoración de metadatos) y publicar **guías de actuación** con carga probatoria y criterios de valoración técnica.

5. **Coordinación con la autoridad de datos.** Integrar la actuación con la autoridad prevista en la Ley Orgánica de Protección de Datos Personales para garantizar derechos y sanciones administrativas complementarias.

5. Salvaguardas y límites (evitar criminalización excesiva)

- **Exclusión de la criminalización de la crítica legítima y el insulto aislado.** El numeral 4 del proyecto evita sancionar expresiones que formen parte del debate público o juicios de valor, garantizando libertad de expresión en los límites constitucionales.
- **Regla de mínima intervención penal.** Priorizar la intervención penal cuando existan indicios de daño real, reiteración y afectación grave a la integridad psíquica; en casos menores, promover remedios civiles, administrativos o medidas restaurativas.
- **Control jurisdiccional estricto.** Todas las medidas de remoción y acceso a datos deben requerir motivación y control judicial para respetar proporcionalidad y protección de datos.

6. Transición y medidas complementarias

- **Disposición transitoria.** Establecer un periodo (ej.: 6 meses) desde la entrada en vigor para elaborar protocolos interinstitucionales, capacitar operadores y definir formularios de denuncia electrónica.
- **Acciones complementarias no penales.** Incentivar políticas educativas (Ministerio de Educación) y protocolos escolares para ciberbullying, reforzando la prevención y la reparación extrajudicial de daños. Colombia y España han combinado tipificaciones

penales con sistemas escolares de convivencia.

7. Argumentos comparados.

- **España (art. 172 ter CP).** Tipifica el acoso (stalking) y permite agravar cuando se usa tecnología; útil como antecedente para la idea de persecución/acecho digital.
- **Colombia (Leyes 1273/2009 y 1620/2013).** Protege datos y derechos escolares; su énfasis ha sido mixto: desarrollo de delitos informáticos y políticas educativas, pero ausencia de un tipo penal autónomo de ciberacoso general (sirve de contraste).
- **México (Ley Olimpia).** Se centra en la violencia digital y la difusión de contenido íntimo; destaca la necesidad de agravantes y medidas de remoción rápida.
- **Chile (Ley 21.153 y reformas).** Penaliza la difusión no consentida de imágenes íntimas y avanza en medidas de protección digital; útil para formular agravantes sobre difusión masiva.

II. PROPUESTA PROCESAL 1

Protocolo obligatorio de investigación de evidencia digital

Propuesta de incorporación: Protocolo nacional de investigación de evidencia digital en casos de ciberacoso

Con el fin de garantizar la eficacia de la persecución penal y la validez probatoria de la evidencia digital en los casos de ciberacoso, se propone la adopción de un **protocolo obligatorio de investigación de evidencia digital**, de aplicación inmediata por parte de la fiscalía general del Estado y los órganos auxiliares de investigación.

Dicho protocolo deberá contemplar, como mínimo, los siguientes estándares técnicos y jurídicos:

a) **Recolección técnica de evidencia digital**, incluyendo metadatos, cabeceras de correo electrónico, direcciones IP, registros de acceso (logs), identificadores de usuario y cualquier otro dato técnico que permita la trazabilidad de la conducta digital;

b) **Cadena de custodia digital**, asegurando la identificación, conservación, traslado, análisis y almacenamiento de la evidencia electrónica mediante procedimientos documentados que garanticen su autenticidad, integridad y no alteración;

c) **Preservación inmediata del contenido digital**, mediante técnicas de sellado criptográfico, utilizando algoritmos de hash seguros (por ejemplo, SHA-256), con el fin de garantizar la inmutabilidad de la evidencia desde el momento de su recolección;

d) **Solicitud urgente de información a plataformas digitales extranjeras**, a través de mecanismos de cooperación judicial, asistencia penal internacional o requerimientos directos previstos en la normativa interna, priorizando la conservación de datos antes de su eliminación automática;

e) **Estándares mínimos para la validez de capturas de pantalla**, que incluyan fecha, hora, URL visible, identificación del perfil o cuenta, dispositivo utilizado y verificación técnica del origen del contenido, evitando su valoración aislada o informal;

f) **Auditoría de integridad de la evidencia digital**, mediante peritajes técnicos periódicos que certifiquen que los archivos digitales no han sido modificados durante el proceso de investigación y juzgamiento.

Este protocolo permitirá reducir la discrecionalidad en la investigación, fortalecer la seguridad jurídica y evitar la exclusión probatoria por defectos técnicos en la obtención de evidencia digital.

III. PROPUESTA PROCESAL 2

Sistema nacional de denuncia electrónica (24/7).

Con el objetivo de garantizar el acceso efectivo a la justicia y la protección inmediata de las víctimas de ciberacoso, se propone la creación de un **sistema nacional de denuncia electrónica, disponible las 24 horas del día**, administrado por el Estado ecuatoriano y articulado con la Fiscalía General del Estado y el sistema judicial.

Esta plataforma permitiría a las víctimas denunciar de forma directa y segura conductas tales como:

- creación y uso de perfiles falsos;
- amenazas digitales;
- difusión de contenido perjudicial o humillante;
- hostigamiento digital reiterado.

El sistema deberá contar, como mínimo, con las siguientes funcionalidades:

a) **Registro de datos de geolocalización**, respetando los principios de proporcionalidad y protección de datos personales, con fines de investigación penal;

b) **Carga directa de archivos digitales**, incluyendo imágenes, videos, audios, mensajes y enlaces, garantizando su preservación inmediata;

c) **Preservación automática de la evidencia digital**, mediante mecanismos técnicos de sellado temporal y hash criptográfico desde el momento de la denuncia;

d) **Interoperabilidad con plataformas digitales**, para facilitar requerimientos urgentes de conservación o retiro de contenido cuando exista riesgo inminente de daño;

e) **Emisión inmediata de medidas de protección provisionales**, tales como prohibición de contacto digital, bloqueo preventivo de cuentas o advertencias judiciales, sujetas a control jurisdiccional posterior.

La implementación de un sistema de denuncia electrónica permitiría superar barreras de acceso a la justicia, reducir la revictimización y responder de manera oportuna a la naturaleza inmediata y expansiva del daño producido por el ciberacoso.

"La propuesta normativa se complementa con medidas procesales y tecnológicas orientadas a garantizar la investigación eficaz de la evidencia digital y el acceso inmediato a la justicia de las víctimas, reconociendo que la tutela penal del ciberacoso exige no solo tipificación, sino también mecanismos probatorios y de protección adecuados al entorno digital."

Propuestas de política criminal: creación de una unidad especializada en violencia digital

Como complemento indispensable a la tipificación penal del ciberacoso y a las medidas procesales propuestas, resulta necesario fortalecer la **capacidad institucional del Estado** para investigar y responder de manera eficaz a la violencia digital. En este sentido, se propone la creación de una **unidad especializada en violencia digital dentro de la Fiscalía General del Estado**.

Dicha unidad deberá contar con un **equipo interdisciplinario especializado**, integrado, como mínimo, por:

- **peritos informáticos**, encargados de la recolección, análisis y preservación de evidencia digital;
- **psicólogos forenses**, responsables de la valoración del daño psíquico, la afectación emocional y la credibilidad del testimonio de las víctimas;
- **analistas de redes digitales**, especializados en la detección de campañas coordinadas, uso de bots, perfiles falsos y dinámicas de hostigamiento masivo;
- **instructores y fiscales especializados**, con formación continua en delitos tecnológicos, prueba digital y derechos fundamentales en el entorno digital.

La función principal de esta unidad será **investigar de manera prioritaria y especializada los casos de ciberacoso**, garantizando una **respuesta inicial en un plazo máximo de setenta y dos (72) horas** desde la recepción de la denuncia, con el fin de evitar la prolongación del daño, la pérdida de evidencia digital y la revictimización.

La creación de una unidad especializada permitiría superar las limitaciones actuales derivadas de la investigación generalista de delitos digitales, fortalecer la seguridad jurídica, mejorar la calidad probatoria y asegurar una tutela efectiva de los derechos de las víctimas de violencia digital, en consonancia con los principios de especialización, eficiencia y protección reforzada que inspiran la política criminal contemporánea.

La eficacia de la propuesta legislativa requiere, además, el fortalecimiento institucional mediante la creación de unidades especializadas en violencia digital, capaces de responder de forma rápida, técnica e interdisciplinaria a los casos de ciberacoso.

Propuesta de armonización del COIP con la Constitución de la República del Ecuador

La Constitución de la República del Ecuador reconoce y garantiza de manera expresa derechos fundamentales directamente afectados por el fenómeno del ciberacoso, tales como la **integridad psíquica** (art. 66.3), la **honra y reputación** (art. 66.8) y el **derecho a la protección de datos personales** (art. 66.19). Estos derechos gozan de protección constitucional autónoma y constituyen bienes jurídicos de máxima jerarquía dentro del ordenamiento jurídico ecuatoriano.

No obstante, el Código Orgánico Integral Penal no ha desarrollado una tutela penal específica e integral de estas garantías en el contexto digital, limitándose a regular de manera fragmentada ciertas conductas tecnológicas sin reconocer expresamente el **ciberacoso como una forma de violencia** que vulnera de manera directa dichos derechos fundamentales. Esta omisión genera una desarmonización entre el marco constitucional y el marco penal, afectando el deber estatal de protección efectiva de los derechos.

En este contexto, se propone **reconocer normativamente al ciberacoso como una forma de violencia que vulnera la integridad psíquica, la honra y la protección de datos personales**, lo cual constituye el fundamento constitucional de la reforma penal planteada.

Dicha declaración no solo cumple una función simbólica, sino que orienta la

interpretación judicial, fortalece el principio de legalidad y legitima la intervención penal frente a conductas de hostigamiento digital reiterado que producen daño psíquico prolongado.

La armonización del COIP con la Constitución permitirá superar la actual fragmentación normativa, garantizar coherencia sistemática del ordenamiento jurídico y asegurar que la respuesta penal frente al ciberacoso se encuentre alineada con los estándares constitucionales de protección reforzada de los derechos fundamentales en el entorno digital.

La reforma penal propuesta se sustenta, además, en la necesidad de armonizar el Código Orgánico Integral Penal con la Constitución de la República, reconociendo al ciberacoso como una forma de violencia que vulnera derechos fundamentales como la integridad psíquica, la honra y la protección de datos personales.

Propuesta de mecanismos de reparación integral en casos de ciberacoso

La respuesta penal frente al ciberacoso no debe limitarse a la imposición de una sanción privativa de libertad, sino que debe orientarse a la **reparación integral del daño causado a la víctima**, en coherencia con los principios constitucionales de tutela efectiva, dignidad humana y justicia restaurativa.

En atención a la naturaleza del daño producido por el ciberacoso —frecuentemente prolongado, público y de difícil reversión—, se propone la incorporación de **mecanismos específicos de reparación integral**, aplicables de manera complementaria a la sanción penal, entre los cuales se incluyen:

a) **Disculpas públicas supervisadas judicialmente**, cuando el daño haya tenido una dimensión pública o masiva, garantizando que dichas disculpas no generen una nueva forma de revictimización ni exposición indebida de la persona afectada;

b) **Retiro permanente, bloqueo o desindexación definitiva del contenido digital lesivo**, incluyendo publicaciones, imágenes, videos o comentarios, mediante orden judicial dirigida a las plataformas digitales correspondientes;

c) **Terapia psicológica ordenada judicialmente**, a cargo del agresor, destinada a la atención del daño psíquico causado a la víctima y, cuando resulte pertinente, a procesos de reeducación y control de impulsos del infractor;

d) **Mecanismos de arrepentimiento activo**, consistentes en la colaboración efectiva del agresor para cesar el hostigamiento, identificar y eliminar réplicas del contenido dañino, abstenerse de nuevas conductas de acoso y participar en procesos restaurativos supervisados.

La implementación de estos mecanismos permitirá una respuesta penal más proporcional, humana y eficaz frente al ciberacoso, contribuyendo no solo a la sanción del infractor, sino también a la restauración de la dignidad, la integridad psíquica y la tranquilidad personal de la víctima.

La propuesta normativa incorpora mecanismos de reparación integral adaptados al entorno digital, reconociendo que la protección efectiva de las víctimas de ciberacoso exige no solo sanción penal, sino también medidas restaurativas orientadas a la recomposición del daño psíquico y social.

PROPUESTA INNOVADORA 1

Sistema de "alerta roja digital"

Implementación de un sistema de alerta roja digital en casos de ciberacoso reiterado

Como mecanismo innovador de protección inmediata frente al ciberacoso, se propone la implementación de un **sistema de "alerta roja digital"**, inspirado en los modelos de respuesta urgente utilizados en casos de violencia de género. Este sistema se activaría cuando la víctima reporte **hostigamiento digital reiterado** que presente indicios razonables de riesgo inminente de daño psíquico grave o escalamiento de la violencia.

La activación de la alerta roja digital permitiría a la Fiscalía General del Estado recibir una **notificación automática prioritaria**, habilitando la adopción inmediata de medidas

urgentes, tales como:

a) **Bloqueo preventivo y temporal de cuentas o perfiles utilizados para el hostigamiento**, mientras se realiza la verificación judicial correspondiente;

b) **Preservación inmediata de la evidencia digital**, incluyendo contenidos, metadatos, registros de acceso y direcciones IP, con el fin de evitar su eliminación o alteración;

c) **Imposición provisional de restricciones digitales**, orientadas a impedir el contacto digital directo o indirecto con la víctima.

Este sistema permitiría una respuesta temprana y eficaz, adecuada a la naturaleza inmediata y expansiva del daño producido por el ciberacoso, reduciendo la revictimización y la pérdida de evidencia.

PROPUESTA INNOVADORA 2

Supervisión judicial del comportamiento digital del agresor.

Como medida complementaria de prevención especial y protección reforzada de la víctima, se propone habilitar la **supervisión judicial del comportamiento digital del agresor**, especialmente en casos de reincidencia, riesgo elevado o incumplimiento de medidas de protección.

Esta supervisión, sujeta a **control judicial estricto y al principio de proporcionalidad**, podrá comprender:

a) **Control de las cuentas digitales utilizadas por el agresor**, incluidas redes sociales, plataformas de mensajería y servicios en línea relevantes;

b) **Monitoreo de intentos de contacto digital con la víctima**, directos o indirectos;

c) **Verificación de intentos de creación de nuevas cuentas** destinadas a eludir medidas judiciales;

d) **Seguimiento de patrones de conducta digital**, exclusivamente en lo

relacionado con la conducta investigada.

La supervisión judicial del comportamiento digital no constituye una sanción autónoma, sino una medida preventiva orientada a evitar la reiteración del daño, proteger a la víctima y garantizar la eficacia de las órdenes judiciales en el entorno digital.

PROPUESTA INNOVADORA 3

Responsabilidad penal y administrativa de plataformas digitales.

Responsabilidad de plataformas digitales por incumplimiento de órdenes judiciales.

Inspirado en modelos europeos de corresponsabilidad en la lucha contra la violencia digital, se propone establecer un **régimen de responsabilidad penal y administrativa para las plataformas digitales** que, de manera injustificada, **incumplan órdenes judiciales de retiro, bloqueo o preservación de contenido** relacionado con casos de ciberacoso.

En estos supuestos, las plataformas podrán ser sujetas a:

a) **Multas económicas proporcionales a la gravedad del incumplimiento y al volumen de usuarios afectados**;

b) **Suspensión temporal del servicio o de funcionalidades específicas**, en caso de incumplimientos reiterados;

c) **Responsabilidad solidaria en la reparación integral**, cuando su omisión haya contribuido de forma directa a la prolongación o agravamiento del daño causado a la víctima.

Este régimen de responsabilidad no pretende criminalizar la actividad empresarial legítima, sino garantizar la **colaboración efectiva de las plataformas digitales con la justicia**, reforzando la eficacia de las decisiones judiciales y la protección de los derechos fundamentales en el entorno digital.

El artículo incorpora propuestas innovadoras como sistemas de alerta temprana digital,

supervisión judicial del comportamiento en línea y corresponsabilidad de plataformas digitales, orientadas a fortalecer una respuesta penal eficaz y adaptada a la complejidad del entorno digital.

CONCLUSIONES

El análisis desarrollado a lo largo del presente artículo permite concluir que el **ordenamiento jurídico penal ecuatoriano no ofrece una respuesta adecuada, coherente ni suficiente frente al fenómeno del ciberacoso**, particularmente en su modalidad **no necesariamente sexual**, caracterizada por el hostigamiento digital reiterado y el daño psíquico prolongado a la víctima.

En primer lugar, se concluye que el **Código Orgánico Integral Penal (COIP)** carece de un **tipo penal autónomo de ciberacoso**, lo que obliga a subsumir estas conductas en figuras penales dispersas y diseñadas para supuestos distintos. Los artículos 154.2, 157, 178, 180 y 229 del COIP regulan conductas vinculadas al uso de tecnologías de la información, pero **ninguno aborda de manera integral el hostigamiento digital reiterado como fenómeno propio**, lo que genera una **fragmentación normativa estructural**.

En particular, el análisis dogmático del **artículo 154.2 COIP** evidencia una limitación relevante, pues la punibilidad del hostigamiento por medios tecnológicos se condiciona a la **finalidad de causar daño a la integridad física o sexual**. Esta exigencia excluye una amplia gama de conductas de ciberacoso que producen **afectaciones psíquicas, emocionales y sociales**, pero que no persiguen un daño físico ni sexual. Como consecuencia, se generan **dificultades de subsunción típica**, que afectan la eficacia del derecho penal y propician escenarios de atipicidad, archivo de denuncias o recalificaciones forzadas.

Asimismo, se concluye que el **artículo 157 COIP**, relativo a la violencia psicológica, no suple este vacío normativo, ya que su ámbito de aplicación se encuentra limitado a

relaciones familiares o contextos de violencia contra la mujer, dejando sin cobertura penal múltiples casos de ciberacoso que se producen fuera de dichas relaciones. Esta restricción normativa resulta incompatible con la realidad del entorno digital, donde el acoso puede provenir de personas sin vínculo previo con la víctima y desplegarse en espacios públicos virtuales.

Desde una perspectiva constitucional, el estudio demuestra una **desarmonización entre el marco penal y la Constitución de la República del Ecuador**. La Constitución reconoce y garantiza derechos directamente afectados por el ciberacoso, como la **integridad psíquica**, la **dignidad humana**, la **honra**, la **intimidad personal** y la **protección de datos personales**. Sin embargo, el COIP no desarrolla una tutela penal específica y eficaz de estos bienes jurídicos en el contexto digital, lo que compromete el deber estatal de protección efectiva de los derechos fundamentales.

Esta desarmonización incide directamente en el **principio de legalidad y taxatividad penal**, en la medida en que la ausencia de un tipo penal claro obliga a los operadores de justicia a extender o forzar la interpretación de normas penales existentes, lo cual resulta contrario a los principios rectores del derecho penal. A su vez, esta situación afecta el **acceso efectivo a la justicia de las víctimas**, quienes enfrentan barreras normativas para la judicialización de conductas que, aunque lesivas y reiteradas, no encajan plenamente en los tipos penales vigentes.

El análisis también permite concluir que las **leyes de control y políticas públicas vigentes en el Ecuador**, como la Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres, la Ley Orgánica de Protección de Datos Personales y los protocolos institucionales sobre violencia digital, reconocen la existencia y gravedad del ciberacoso, pero **no han sido armonizadas de manera suficiente con el derecho penal**. Esta falta de coordinación normativa refuerza el carácter fragmentado de la respuesta estatal frente a la violencia digital.

En consecuencia, se concluye que la **ausencia de un tipo penal autónomo de ciberacoso en el COIP constituye un déficit normativo relevante**, que limita la función preventiva, protectora y sancionadora del derecho penal ecuatoriano. Este déficit no solo afecta a las víctimas individuales, sino que debilita la capacidad del Estado para responder de manera adecuada a una forma contemporánea de violencia que se ha intensificado con el uso masivo de tecnologías digitales.

Finalmente, el estudio confirma la **necesidad jurídica y constitucional de una reforma normativa**, orientada a incorporar una figura penal específica o un marco penal integral que reconozca el ciberacoso como una conducta autónoma, centrada en el **hostigamiento digital reiterado y el daño psíquico**, y que se articule de manera coherente con la Constitución de la República, el principio de legalidad y las exigencias del entorno digital actual. Solo a través de una respuesta penal clara y sistemática será posible garantizar una protección efectiva de los derechos fundamentales y un acceso real a la justicia para las víctimas de ciberacoso en el Ecuador.

TABLA FINAL DE OPERACIONALIZACIÓN (DETALLADA)

Objetivo Específico	Qué se puede medir	Por qué es viable	Por qué es concreto	Relación con el objetivo general
1. Identificar normas del COIP	Cantidad de artículos analizados (154.2, 157, 178, 180, 229)	Está en un solo cuerpo legal accesible	Se limita al COIP	Permite detectar brechas
2. Comparar con Constitución	Correspondencia artículo por artículo	Son normas públicas	Limita análisis a 3 derechos	Evalúa coherencia normativa
3. Revisar doctrina/jurisprudencia	Nº de textos, tesis, protocolos revisados	Repositorios públicos	Solo violencia digital	Identifica vacíos prácticos
4. Comparar con Colombia	Nº de similitudes/diferencias	Información pública	Solo un modelo de referencia	Soporta propuestas
5. Proponer lineamientos	Propuesta concreta redactada	Requiere solo análisis jurídico	Basado en dos leyes clave	Cierra el análisis con soluciones

CRONOGRAMA.

Actividad	Seman a 1	Seman a 2	Seman a 3	Seman a 4	Seman a 5	Seman a 6
Revisión bibliográfica y estado del arte	X	X				
Análisis del marco normativo nacional (Código Orgánico Integral Penal. (COIP))		X	X			
Revisión de jurisprudencia nacional (Corte Nacional y Corte Constitucional)			X	X		
Análisis de derecho comparado (España, México, Colombia y Chile)			X	X		
Construcción de la matriz de análisis (primacía de la realidad, subordinación, etc.)				X	X	
Aplicación de Doctrina				X	X	
Análisis de resultados (documentales y de campo)					X	
Análisis comparado					X	
Elaboración del marco teórico y discusión					X	
Redacción del informe Final						X
Revisión final y entrega del anteproyecto						X

Referencias Bibliográficas.

Alexandra, Z. V. (JULIO-2021). CIBERACOSO;CYBERBULLYING;PRINCIPIO DE LEGALIDAD;DERECHOS HUMANOS. *UNIANDES*, 23.

Anibal, B. C. (Diciembre-2023). CIBERACOSO;DELITOS INFORMÁTICOS;MEDIDAS DE PROTECCIÓN;COIP;TECNOLOGÍAS. *UNIANDES*, 1-28.

ART. 154.2 COIP, R. D. (2014). ART. 154.2, CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP. *LEXISFINDER*, 1-297.

ART. 157 COIP, R. D. (2014). CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP. *LEXISFINDER*, 1-297.

ARTS. 173 & 174 COIP, R. D. (2014). CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP.

LEXISFINDER, 1-297.

ARTS.66.3&66.8&66.19CRE, C. D. (2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. *LEXISFINDER*, 1-219.

Barreto CAlderón, O. (. (2024). El ciberacoso en Ecuador. *El ciberacoso en Ecuador: análisis comparado con la legislación española*. Milagro, Guayas, Ecuador: Repositorio Institucional.

Barreto, O. C. (2024). El ciberacoso en Ecuador: Análisis comparado con la Legislación Española. *UNEMI*, 3.

Censos, I. N. (2023). *nstituto Nacional de Estadística y Censos. (2023). Tecnologías de la información y comunicación (TIC) en hogares ecuatorianos.* Guayaquil,Ecuador.

Consumidor, P. F. (26 de Abril de 2021). *Gobierno de México.* Obtenido de Gobierno de México: https://www.gob.mx/profeco/articulos/la-ley-olimpia-y-el-combate-a-la-

violencia- digital?idiom=es#:~:text=%C2%BFCu%C3%A1les%20son%20las%20sanciones?,C%C3%B3mo%20mantener%20chats%20m%C3%A1s%20seguros?

CRE, C. D. (2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. *LEXISFINDER*, 1-219.

digital, A. (2023). España. (2023). Código Penal (art. 172 ter). *Agencia Estatal Boletín Oficial del Estado.* Barcelona, España.

digital, V. s. (2014). Ecuador. (2014). Código Orgánico Integral Penal. *Registro Oficial Suplemento No. 180.* Quito, Pichincha, Ecuador.

Elizabeth, T. A. (Febrero - 2023). VIOLENCIA DIGITAL;CYBERBULLYING RED SOCIAL. *UNIANDES*, 1-27.

Est.Español, A. E. (2024). *Ley del Código Penal.* Madrid: Agencia Estatal Boletín Oficial del Estado.

Estado, F. G. (Agosto de 2015). *Fiscalía General Del Estado.* Obtenido de Fiscalía General Del Estado: https://www.fiscalia.gob.ec/a-un-ano-del-coip-la-fiscalia-refuerza-su-trabajo-investigativo

Ley 1273, L. 1.-C. (2009). Ley 1273 de 2009. *Departamento Administrativo de la Función Pública*, 1-3.

Ley 1620, L. 1.-C. (2013). Ley 1620 de 2013. *Departamento Administrativo de la Función Pública*, 1-15.

Ley 21153, M. D. (2019). Ley 21153. *Biblioteca del Congreso Nacional de Chile*.

Penal, C. O. (2014). *https://www.asambleanacional.gob.ec*. Obtenido de Registro Oficial Suplemento No. 180.

Penal, E. (. (2014). *Asamblea Nacional del Ecuador*. Obtenido de https://www.asambleanacional.gob.ec.

Pozo Chugá, V. E. (2025). Acciones necesarias para hacer frente al acoso digital en el

Ecuador. *Revista Sociedad & Tecnología, 8(2)*, 1-12.

Pozo, V. E. (01/05/2025). Acciones necesarias para hacer frente al acoso digital en la. *Revista científica Sociedad & Tecnología*, 1-12.

Tamara, J. S. ((2018)). Ciberbullying como delito informático en el Derecho Penal Ecuatoriano. *UNIVERSIDAD CENTRAL DEL ECUADOR*, 1-145.

Zúñiga Vásquez, A. (. (2021). Ciberacoso, cyberbullying y principio de legalidad penal en el Ecuador [Tesis de grado, Universidad Regional Autónoma de los Andes]. .

Repositorio institucional.

PRESUPUESTO.

PRESUPUESTO PARA GASTOS POR INVESTIGACIÓN		
	RECURSOS	VALOR
CONCEPTO.	Plan de Internet/ Datos del celular	$60
	Lápiz/Borrador	$0,75
	Cuaderno a cuadros	$1,50
	Movilización hacía	$200
	Micrófonos de solapa	$30
	Alimentación personal	$300
	Impresiones varias	$100
	Servicios de electricidad, internet, telefonía	$120
	Alimentación/ Snacks	$345
	Movilización a las cabinas de la Universidad Politécnica Salesiana para grabar las voces principales	$200
	Ordenador PHPPAvilon 4 generación Ram 16, H/D 1TB	$1.800
	TOTAL	$3.157,25