



Revista de Derecho Directum. Vol. 3, No. Especial, pp. 12-25. Octubre 2026
ISSN: 3028-8754. ISSN Elect. 3028-8762. Universidad Católica de Cuenca

La relación del derecho penal con la ciberviolencia y la ciberpaz

The Relationship of Criminal Law with Cyberviolence and Cyberpeace

Recepción: 10 de junio de 2026

Revisión: 20 de julio de 2026

Aceptación: 28 de agosto de 2026

Publicación: 2 de octubre de 2026

Diana Cecilia González Maldonado

Universidad Católica de Cuenca

dcgonzalezm@ucacue.edu.ec

<https://orcid.org/0000-0003-2973-4967>



Francisco Javier Gorjón Gómez

Universidad Autónoma de Nuevo León

francisco.gorjon@uanl.mx

<https://orcid.org/0000-0001-5296-6454>



<https://doi.org/10.26871/directum.v3.nSI.59>

Cita sugerida:

González Maldonado, D. C., y Gorjón Gómez, F. J. (2026). La relación del derecho penal con la ciberviolencia y la ciberpaz. *Revista de Derecho Directum*, 3(esp.), 12-25. DOI: <https://doi.org/10.26871/directum.v3.nSI.59>

Resumen

En el trabajo se analiza la relación entre el derecho penal, la ciberviolencia y la promoción de la ciberpaz dentro del entorno digital. Se destaca que las innovaciones tecnológicas han facilitado la comunicación y la accesibilidad a la información en el entorno digital y la generación de nuevas formas de violencia en línea que se han convertido en una amenaza a los derechos fundamentales como la dignidad, la intimidad y la seguridad. Para abordar estos desafíos, el derecho penal debe evolucionar por medio de la revisión y actualización constante de la normativa, garantizando sanciones proporcionales y efectivas, pero también promoviendo acciones preventivas, educativas y de protección a las víctimas. La importancia de la promoción de una cultura de paz digital apoyada en el respeto y la responsabilidad es un elemento clave para la reducción de conductas delictivas, por lo que la intervención estatal debe estar encaminada a la búsqueda de un equilibrio entre sancionar y prevenir, evitando el uso excesivo del sistema penal y fomentando entornos digitales seguros que fortalezcan la convivencia pacífica y la protección de los derechos humanos en la era digital.

Palabras clave: derecho penal, ciberviolencia, ciberpaz, criminalización, entorno digital.

Abstract

This article analyzes the relationship between criminal law, cyberviolence, and the promotion of cyberpeace within the digital environment. It highlights how technological innovations have facilitated communication and access to information while also giving rise to new forms of online violence that threaten fundamental rights such as dignity, privacy, and security. To address these challenges, law must evolve through the constant review and updating of regulations, ensuring sanctions are both proportionate and effective while also promoting preventive, educational, and victim-protection measures. Fostering a culture of digital peace grounded in respect and responsibility is key to reducing criminal behavior; therefore, state intervention should aim to strike a balance between punishment and prevention, avoiding over-reliance on the penal system and instead fostering safe digital environments that strengthen peaceful coexistence and the protection of human rights in the digital age.

Keywords: Criminal Law, Cyberviolence, Cyberpeace, Criminalization, Digital Environment.

Introducción

La tecnología ha modificado la manera en la que nos comunicamos, interactuamos y vivimos; su expansión ha generado cambios en la sociedad en su dinámica económica, social y cultural. Este cambio tecnológico ha beneficiado a la sociedad por el fácil acceso a la información, por permitir una conectividad a nivel global y por la liberalización de diversas expresiones sociales y culturales. A pesar de ello, de forma simultánea a estos avances se han desarrollado nuevas formas de violencia y delincuencia que en el ámbito digital se conocen como ciberviolencia, las mismas que se han convertido en una amenaza para la paz y la seguridad en el ámbito digital y que afectan de forma directa a la ciberpaz.

En este contexto, surgen fenómenos como el ciberacoso, la difusión no consentida de contenidos íntimos, el *grooming*, el *ciberbullying*, entre otras formas de ciberviolencia que tienen un efecto negativo en los derechos fundamentales como la dignidad, la intimidad, la libertad y la seguridad de los individuos, lo que evidencia que este tipo de conductas ocasiona daños psicológicos y sociales con consecuencias éticas y legales para los usuarios del entorno digital.

En Ecuador, la respuesta jurídica frente a la ciberviolencia aún presenta limitaciones. Aunque el Código Orgánico Integral Penal sanciona conductas como el acoso, la violación a la intimidad y diversos delitos informáticos, manifestaciones específicas como el ciberacoso no cuentan con una tipificación penal autónoma, lo que dificulta su investigación y sanción (Teijón Alcalá, 2023). A ello se suma una regulación dispersa entre distintas normas, sin un mecanismo interinstitucional que articule de manera integral la respuesta frente a estas conductas.

Ante esta realidad, el estudio analiza la relación entre el derecho penal, la ciberviolencia y la ciberpaz, con el propósito de identificar los principales vacíos normativos y proponer un mecanismo articulado de tipificación, sanción y prevención, reconociendo que el derecho penal constituye una parte de la respuesta y debe complementarse con políticas públicas y estrategias preventivas.

Desarrollo

Relación del derecho penal con la ciberviolencia y la ciberpaz

El entorno digital se ha convertido en un sitio en el que interactúan los individuos de forma individual o multitudinaria donde las personas se conectan, comparten y crean contenido. En ese mismo entorno también en muchas ocasiones las personas han tenido experiencias agresivas y violentas que impactan en su vida personal y social, lo que se conoce como ciberviolencia. Frente a esta situación, la ciberpaz propone un entorno digital basado en el respeto y la prevención. En este escenario, el derecho penal cumple su función de sancionar conductas delictivas, pero también de proteger los derechos fundamentales y contribuir a una convivencia digital pacífica, actuando como una herramienta coercitiva que es utilizada para imponer orden y controlar el comportamiento de los individuos (López Gorostidi, 2022).

Es importante indicar que el aporte del derecho penal a una convivencia más pacífica no significa que su función principal sea prevenir los conflictos. Su finalidad es, ante todo, sancionar aquellas conductas que previamente han sido reconocidas por la ley como delitos, respetando el principio de legalidad establecido en el artículo 76 de la Constitución de la República del Ecuador de 2008. En este contexto, el derecho penal debe enfrentarse a retos que provienen de las características propias del entorno digital, donde se necesitan normas claras para responder de forma adecuada y proporcional a las conductas delictivas que se presentan; en este sentido, las políticas públicas y las estrategias de prevención deben orientarse a la reducción de la violencia en línea y a la mejora de la convivencia pacífica en el ámbito digital. Estas medidas deben trabajar de manera coordinada con la respuesta penal, pero sin confundir sus funciones, manteniendo a la sanción como una medida de última instancia (Ferrajoli, 2018).

Según Camere Figueroa (2022), el derecho penal es considerado como un conjunto de normas que el Estado establece para sancionar las conductas que perjudican la convivencia de la sociedad, mediante el establecimiento de penas a quienes incumplen la normativa. En este sentido, el derecho penal está encaminado a la protección de los derechos fundamentales de la sociedad al actuar como un instrumento que contribuye al desarrollo de la paz social y a conservar el orden de la comunidad.

Así también, el derecho penal sanciona los comportamientos que afectan a la coexistencia de las personas considerando el principio de legalidad que establece que la ley es la que define qué actos son considerados como delitos y qué penas deben imponerse, lo que garantiza que los individuos sean sancionados conforme al principio

de proporcionalidad. En este mismo sentido, es importante indicar que la intervención penal debe ser de *ultima ratio*, es decir, que solo debe aplicarse cuando otros mecanismos jurídicos y sociales no sean suficientes, respetando los principios de legalidad, proporcionalidad y culpabilidad (Ferrajoli, 2018).

Para comprender la relación, la tabla 1 presenta una comparación entre las perspectivas de diferentes autores considerando la relación de la ciberviolencia, el rol que cumple el Estado, el enfoque criminológico y los riesgos de esta relación, con el siguiente detalle:

Tabla 1

Tabla comparativa de las perspectivas sobre el derecho penal y la ciberviolencia: Jakobs, Ferrajoli y Zaffaroni

Autor	Modelo y enfoque del derecho penal	Relación con la ciberviolencia	Rol del Estado	Enfoque criminológico	Riesgos
Jakobs	Funcionalismo sistémico. Distingue entre <i>derecho penal del ciudadano</i> y <i>derecho penal del enemigo</i> .	Riesgo sistémico que requiere respuestas punitivas reforzadas. La ciberviolencia grave (como el ciberterrorismo o el abuso sexual sistemático en línea) puede considerarse una amenaza estructural al orden social. Justifica medidas excepcionales frente a los “enemigos” del sistema jurídico.	El Estado debe neutralizar peligros futuros, incluso con medidas anticipadas o limitación de garantías, cuando el sujeto desconoce el orden normativo.	Funcionalismo sistémico: la norma se reafirma con la pena	Pérdida de garantías, criminalización anticipada. Se cuestiona la compatibilidad con el Estado de derecho.

Autor	Modelo y enfoque del derecho penal	Relación con la ciberviolencia	Rol del Estado	Enfoque criminológico	Riesgos
Ferrajoli	Garantismo penal (<i>ultima ratio</i>) y debe estar sometido estrictamente a los principios constitucionales.	Lesión de bienes jurídicos que debe ser penalizada legal y proporcionalmente. La ciberviolencia debe enfrentarse con leyes claras, precisas y estrictamente necesarias. Rechaza el uso del derecho penal como herramienta simbólica o anticipatoria.	El Estado debe actuar dentro de los límites constitucionales, protegiendo derechos fundamentales y evitando la criminalización excesiva.	Criminología de los derechos humanos	Populismo punitivo, ampliación del sistema penal. Crítica la tendencia punitivista y la ampliación de figuras penales ambiguas que afectan garantías individuales.
Zaffaroni	Crítica al sistema penal moderno. Ve al derecho penal como parte de un sistema selectivo que reproduce desigualdad.	Expresión de conflicto estructural y desigualdad social. Advierte que la penalización de la ciberviolencia puede derivar en una nueva forma de control punitivo, especialmente sobre sectores vulnerables. Aboga por respuestas integrales (educación, prevención).	El Estado debe evitar el abuso del sistema penal como única respuesta al conflicto. Propone una reforma estructural del sistema.	Criminología crítica/abolicionista	Uso simbólico del castigo, criminalización de lo vulnerable. Señala el riesgo de criminalización simbólica, populismo penal y pérdida del sentido humanista del derecho penal.

La tabla resume tres modelos de respuesta penal frente a la ciberviolencia: el funcionalismo sistémico de Jakobs, que acepta respuestas punitivas reforzadas frente a riesgos sistémicos graves; el garantismo penal de Ferrajoli, que exige que la respuesta penal sea legal, proporcional y estrictamente necesaria; y la criminología crítica de Zaffaroni, que advierte sobre el riesgo de un uso simbólico y desigual del castigo.

El incremento de la ciberviolencia requiere que el derecho penal en la actualidad actúe de forma efectiva al brindar respuestas adecuadas para que no se vulneren los principios del Estado de derecho; en este sentido, Jakobs defiende al derecho penal del enemigo para contrarrestar a quienes amenazan al orden jurídico; Ferrajoli, por su parte, plantea un modelo garantista que se centra en la legalidad, la proporcionalidad y el respeto de los derechos fundamentales; mientras que Zaffaroni advierte sobre el uso excesivo del castigo como una forma de control social y defiende soluciones estructurales más allá de lo punitivo. Si se comparan estos criterios, se pueden comprender las tensiones entre seguridad y libertad en el ámbito digital, a pesar de que el derecho penal pueda responder a los delitos tecnológicos sin caer en la impunidad ni en el autoritarismo y que su aplicación sea justa y respetuosa con la dignidad humana.

En la era digital, el derecho penal ha tenido que adaptarse a la realidad actual, como la ciberviolencia, entendida como toda forma de agresión desarrollada en el ámbito digital; este tipo de comportamiento se hace evidente por medio del acoso, amenazas y agresiones que se presentan en las plataformas digitales, lo cual se convierte en un reto para el sistema de justicia penal (Agustina, 2021). Por lo tanto, hay que considerar que la ciberviolencia hace evidente la necesidad de incorporar un marco legal robusto que contribuya a la prevención y a la sanción de las conductas criminales que se desarrollan en el entorno digital y que afectan de forma psicológica y física a los individuos que interactúan en el entorno.

La relación del derecho penal con la ciberviolencia y la ciberpaz es un tema relevante en la actualidad, por el desarrollo de las tecnologías digitales que han transformado las formas de comunicarse de los individuos, lo que ha originado la manifestación de nuevas formas de violencia digital conocidas como ciberviolencia, que perjudican la convivencia social y los derechos fundamentales como la dignidad, la seguridad y la privacidad. Ante esta realidad, el derecho penal ofrece respuestas que no solo estén enfocadas a la sanción, sino que también contribuyan a la prevención de conductas violentas en línea. Para ello, es indispensable que las leyes se adapten a las nuevas realidades tecnológicas, promoviendo la creación de normativas específicas que permitan identificar estas conductas, investigar los casos y establecer las sanciones correspondientes (Cámara Arroyo, 2020). El derecho penal debe actuar de forma responsable, evitando el uso excesivo de la pena mientras promueve la cultura de paz en los entornos digitales, fomentando el respeto, la responsabilidad y la ética en el uso de las tecnologías.

Caso ecuatoriano: marco normativo fragmentado

El derecho penal y la ciberviolencia pueden ser analizados de diferentes maneras, en función de cómo el derecho penal aplica la normativa a las conductas delictivas en el entorno digital y cómo puede convertirse en una herramienta para erradicar este problema (Teijón Alcalá, 2023). En Ecuador la respuesta jurídica frente a la ciberviolencia no se encuentra concentrada en una sola norma, sino que se aborda desde diferentes disposiciones legales que permiten actuar frente a determinadas conductas que ocurren en los entornos digitales.

En este contexto, el Código Orgánico Integral Penal (COIP, 2014) contempla la sanción de conductas como el acoso, que puede presentarse también a través de medios digitales, así como aquellas que vulneran la intimidad de las personas y otros delitos relacionados con el uso de las tecnologías. A estas conductas se suman acciones que pueden afectar la honra y la reputación de una persona y que, debido al uso cotidiano de redes sociales y otros espacios digitales, también pueden producirse y difundirse a través de estos medios (Teijón Alcalá, 2023). De esta manera, aunque la legislación ecuatoriana ofrece mecanismos para responder ante diferentes manifestaciones de violencia en línea, su tratamiento jurídico se encuentra distribuido entre distintas figuras y disposiciones normativas.

Así también, la Ley Orgánica de Comunicación regula la comunicación digital y establece principios para la protección de la honra y la imagen de los individuos (Ley Orgánica de Comunicación, 2019). Esta normativa considera medidas que prohíben la difusión de la información falsa que atente a la dignidad de las personas. Por su parte, la Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres reconoce a la ciberviolencia como una forma de violencia que afecta a las mujeres y establece medidas específicas para su prevención y sanción (Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres, 2018).

Por su parte, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece un marco legal para la protección de datos personales donde se regula la recopilación, uso, divulgación y transferencia de datos personales del sector público y privado; esta normativa considera principios como la licitud, la finalidad, la minimización de datos y la transparencia para asegurar la privacidad y el buen uso de la información personal (LOPDP, 2021). De esta manera, el derecho penal no solo debe considerarse como un pilar fundamental en la conservación del orden social y la defensa de los derechos fundamentales, sino que se enfrenta al desafío que representa la ciberviolencia en la sociedad digital actual.

Esta situación permite observar una de las principales limitaciones del marco jurídico ecuatoriano frente a la ciberviolencia. Al no existir una tipificación específica del ciberacoso, su tratamiento penal debe apoyarse en otras figuras jurídicas que no fueron creadas originalmente para responder a las particularidades de las conductas desarrolladas en los

entornos digitales. Esto puede generar dificultades al momento de determinar la figura penal aplicable, reunir las pruebas necesarias y llevar adelante el proceso penal, lo que también puede afectar la respuesta que reciben las víctimas (Álvarez Rodríguez, 2020).

Con el objetivo de promover el concepto de ciberpaz y de crear un entorno digital que sea seguro y respetuoso, las normas penales deben evolucionar de forma simultánea para contribuir al establecimiento de mecanismos de prevención y sanción que fomenten la convivencia armónica en el entorno para la protección de los derechos fundamentales y la promoción de la justicia social.

De esta manera, la relación entre el derecho penal y la ciberpaz es importante para la promoción de un ambiente pacífico y sin violencia, donde los individuos puedan interactuar sin sufrir ningún tipo de agresión (Gómez Pilco, 2020); la protección de las víctimas de delitos cibernéticos requiere identificar factores de riesgo, proporcionar apoyo y favorecer su recuperación por medio de un enfoque proactivo que permita investigar los crímenes. El derecho penal, al tipificar y sancionar conductas en el ámbito digital, juega un rol importante en la prevención de este tipo de comportamientos inclusive desde un enfoque criminológico para lograr la concienciación sobre el uso responsable de la tecnología.

Teorías criminológicas para la comprensión de la ciberviolencia

Las teorías criminológicas ofrecen marcos conceptuales importantes para la comprensión de la dinámica de la ciberviolencia y el diseño de estrategias efectivas tanto punitivas como preventivas. Entre ellas se destacan la teoría de las actividades cotidianas y la teoría del aprendizaje social, que permiten analizar las causas y la configuración de los delitos en el ámbito digital, así como la manera de orientar las acciones del derecho penal y las políticas públicas hacia la promoción de la ciberpaz y la defensa de los derechos humanos.

Teoría de las actividades cotidianas en el ámbito digital

La teoría de las actividades cotidianas, que fue originalmente propuesta para explicar la ocurrencia de los delitos en contextos tradicionales, ha sido aplicada para demostrar cómo ciertas prácticas facilitan el cometimiento de delitos informáticos. Según Cohen y Felson (1979), esta teoría aplicada al ámbito digital muestra que los delitos se presentan cuando se agrupan tres factores: alguien con la intención de hacer daño, un individuo vulnerable y los escasos mecanismos de protección.

Esto, en el entorno digital, demuestra que se desarrollan prácticas donde no se aplican medidas de seguridad, se comparte información sin filtros y se interactúa en espacios sin vigilancia adecuada, situaciones que facilitan el desarrollo de conductas delictivas como el

ciberacoso o la publicación de información no consentida; estas circunstancias favorecen el desarrollo de delitos como el ciberacoso, la difusión no consentida de contenidos, el *grooming* y otros comportamientos delictivos que ponen en riesgo la integridad y la dignidad de los individuos.

En este contexto, se evidencia que la mayoría de las conductas delictivas que se desarrollan en el ámbito digital surgen no solo por la malicia de los actores, sino también por la presencia de contextos vulnerables y la falta de mecanismos efectivos de protección y vigilancia. En este contexto, la respuesta frente a estas conductas no debe limitarse al ámbito penal. La teoría de las actividades cotidianas permite reconocer la importancia de complementar la sanción con medidas preventivas orientadas a reducir las oportunidades y los factores de riesgo presentes en el entorno digital. Para ello, pueden desarrollarse campañas de sensibilización sobre el uso responsable de la tecnología, medidas de seguridad digital y procesos educativos que fortalezcan las capacidades de los usuarios para desenvolverse de manera segura en estos espacios.

Teoría del aprendizaje social y la construcción de conductas violentas en el entorno digital

La teoría del aprendizaje social, formulada por Bandura (1971), indica que gran parte de los comportamientos violentos desarrollados en el entorno digital se adquieren y fortalecen en varios grupos o comunidades digitales y no nacen de manera innata. Los individuos, especialmente los jóvenes, observan, reproducen y adquieren conductas agresivas o discriminatorias en redes sociales, foros, chats o plataformas *online*, donde estas prácticas pueden ser normalizadas o incluso reforzadas por medio de la aprobación social, la imitación de modelos que influyen o la exposición a contenidos violentos.

Esta teoría aplicada al contexto del derecho penal en el ámbito digital evidencia cómo la mayoría de las conductas violentas o delictivas en línea no son innatas, sino que se adquieren y fortalecen por medio de las interacciones en diferentes grupos y comunidades digitales. Considerando este punto de vista, el cometimiento de delitos como el ciberacoso, la distribución de contenido no autorizado o el *ciberbullying* puede ser el resultado de la interiorización de conductas que se refuerzan dentro de estos entornos, donde la aprobación social, la influencia de ciertos modelos y la exposición a contenidos violentos son estímulos que fomentan la repetición de este tipo de conductas (Gorjón Gómez, 2024).

Desde este enfoque, la respuesta penal hacia las conductas violentas o delictivas que se desarrollan en los entornos digitales requiere de estrategias preventivas que intervengan en la comunidad donde estos comportamientos pueden desarrollarse y normalizarse. Al respecto, la teoría del aprendizaje social contribuye a resaltar la importancia de la implementación de programas de educación y sensibilización digital que permitan la promoción de modelos de convivencia apoyados en el respeto, la empatía y el reconocimiento de los derechos de los individuos. Estas acciones son las que conciernen al ámbito de las políticas

públicas y de la prevención social, mientras que el derecho penal conserva su función de intervenir cuando se desarrollen aquellas conductas que han sido tipificadas como delitos.

La protección de las víctimas de delitos cibernéticos demanda la creación de un marco legal que permita garantizar la confidencialidad, el apoyo psicológico y su recuperación integral y el restablecimiento de sus derechos; es indispensable el desarrollo de un enfoque proactivo en la investigación de delitos cibernéticos donde la capacitación, educación y concienciación digital son elementos esenciales que contribuyen a fomentar una cultura de ciberpaz (Cámara Arroyo, 2020). En este marco, es indispensable la revisión y actualización de la normativa penal para dar respuesta a las conductas delictivas que se presentan en los entornos digitales y garantizar sanciones proporcionales y respetuosas de los derechos fundamentales.

Propuesta de un mecanismo articulado de respuesta frente a la ciberviolencia

A partir del análisis realizado, es necesario fortalecer la manera de responder a la ciberviolencia a través de acciones que integren el ámbito jurídico, institucional y preventivo. La propuesta está orientada a aprovechar los mecanismos existentes y favorecer una actuación coordinada de las instituciones involucradas frente a las conductas violentas que se producen en el ámbito digital. La propuesta se estructura en cuatro componentes:

1. El primero corresponde a la *tipificación específica del ciberacoso*, que permitirá identificar las conductas violentas y establecer sanciones proporcionales a su gravedad; en el caso ecuatoriano, esto contribuye a la reducción de la dependencia de figuras penales que no siempre responden a las características propias de las conductas desarrolladas en el espacio digital.
2. El segundo componente plantea *fortalecer la coordinación interinstitucional*, por medio del establecimiento de un protocolo que incluya criterios comunes para la recepción de denuncias, investigación de los hechos, protección de las víctimas y tratamiento de los casos de ciberviolencia con el propósito de lograr una actuación articulada de las instituciones involucradas.
3. El tercer componente se refiere a *la gestión de la evidencia digital*, que permita investigar los hechos que se desarrollan en las plataformas tecnológicas y en dispositivos mediante el establecimiento de criterios técnicos para su obtención, conservación y valoración y que puedan servir como elementos probatorios.

4. El cuarto componente se refiere a *la prevención y la educación digital*, acciones complementarias que difieren de la función sancionadora del derecho penal. Estas acciones deben desarrollarse desde las políticas públicas y las instituciones educativas a través de la implementación de programas orientados al uso responsable de las tecnologías, la identificación de riesgos y la promoción del respeto, la empatía y la convivencia pacífica en los espacios digitales.

La propuesta integra la tipificación, la coordinación institucional, el manejo de la evidencia digital y la prevención para dar respuesta de manera integral a la ciberviolencia; su propósito es el fortalecimiento de la actuación del Estado sin extender innecesariamente el poder punitivo, sino con el apoyo de políticas públicas, educación digital y prevención social orientadas a la construcción de una cultura de ciberpaz.

Conclusiones

Es necesario que el derecho penal evolucione y sea capaz de enfrentar a las nuevas formas de violencia que se exhiben en el ámbito digital y que amenazan la convivencia social y la dignidad humana. Este cometido se lleva a cabo por medio de la revisión continua de la normativa y de la adaptación de esta a las nuevas realidades, ya que no se trata solamente de castigar a quienes cometen delitos en este ámbito, sino que también se deben implementar medidas que permitan prevenir estos comportamientos y ofrezcan apoyo a las víctimas.

La relación entre la ciberpaz y el derecho penal involucra la existencia de un equilibrio entre la seguridad y la libertad individual. Según Jakobs, Ferrajoli y Zaffaroni, existen varios enfoques sobre cómo se debería responder ante la presencia de la ciberviolencia, por lo que es necesario un sistema que no solo defienda los derechos fundamentales de las personas, sino que prevenga las conductas delictivas y garantice que las respuestas a los delitos digitales sean adecuadas y justas.

Las teorías criminológicas, como la de las actividades cotidianas y el aprendizaje social, ofrecen información relevante para la comprensión de las causas de la ciberviolencia y el diseño de estrategias efectivas. La aplicación de estas teorías puede contribuir a la implementación de medidas preventivas y punitivas más adecuadas a la realidad digital. Es imprescindible que la normativa se actualice constantemente y que considere las conductas violentas en línea y que la normativa también garantice la aplicación de los principios de legalidad y proporcionalidad, de modo que no solamente se dé prioridad a la sanción, sino a la prevención, a la promoción de valores éticos y a la protección de víctimas en el entorno digital.

Para disminuir la ciberviolencia se requiere una respuesta que no se limite al ámbito penal, sino que se articule con políticas públicas orientadas a la educación digital, la prevención social y la protección de las víctimas de delitos digitales, para dar respuesta a las manifestaciones violentas en línea sin tener que acudir al sistema penal y aportar a la construcción de una cultura de paz y de entornos virtuales seguros y respetuosos.

Referencias bibliográficas

- Agustina, J. R. (2021). Nuevos retos dogmáticos ante la cibercriminalidad. *Estudios Penales y Criminológicos*, 41, 705-777. <https://doi.org/10.15304/epc.41.7433>
- Álvarez Rodríguez, I. (2020). El derecho del ciberespacio. Una aproximación. *IDP. Revista de Internet, Derecho y Política*, (30), 1-13. <https://doi.org/10.7238/idp.v0i30.3201>
- Bandura, A. (1971). *Social learning theory*. General Learning Press.
- Cámara Arroyo, S. (2020). Estudios criminológicos contemporáneos (IX): La cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, (60), 470-512. <https://dialnet.unirioja.es/servlet/articulo?codigo=7524987>
- Camere Figueroa, E. M. (2022). De nuevo, el derecho penal del enemigo: una necesidad para asegurar las condiciones de juridicidad. *Derecho Penal y Criminología*, 44(116), 65-93. <https://doi.org/10.18601/01210483.v44n116.04>
- Código Orgánico Integral Penal. (2014, 10 de febrero). Registro Oficial N.º 180, suplemento. <https://www.asambleanacional.gob.ec/es/system/files/document.pdf>
- Cohen, L. E. y Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-608. <https://doi.org/10.2307/2094589>
- Constitución de la República del Ecuador. (2008, 20 de octubre). Registro Oficial N.º 449.
- Ferrajoli, L. (2018). *Derecho y razón: Teoría del garantismo penal*. Trotta.
- Gómez Pilco, E. L. G. (2020). Ineficiencia del sistema penal en el incremento de la criminalidad. *Ius Vocatio*, 3(3), 93-112. <https://doi.org/10.35292/iusVocatio.v3i3.436>
- Gorjón Gómez, F. J. (Coord.). (2024). *Universidades de paz: La ciencia como precursora de paz*. Universidad Autónoma de Nuevo León.
- Jakobs, G. (1997). *Derecho penal. Parte general: Fundamentos y teoría de la imputación*. Marcial Pons.
- Jakobs, G. y Cancio Meliá, M. (2003). *Derecho penal del enemigo*. Civitas.
- Ley Orgánica de Comunicación. (2019). <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/01/Ley-Organica-de-Comunicación.pdf>
- Ley Orgánica de Protección de Datos Personales. (2021, 26 de mayo). Registro Oficial N.º 459, quinto suplemento. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

- Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres. (2018). https://www.igualdad.gob.ec/wp-content/uploads/downloads/2018/05/ley_prevenir_y_erradicar_violencia_mujeres.pdf
- López Gorostidi, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. *Revista Chilena de Derecho y Tecnología*, 11(1), 121-146. <https://doi.org/10.5354/0719-2584.2022.60913>
- Teijón Alcalá, M. (2023). Los delitos de peligro en el derecho penal contemporáneo. *Revista Electrónica de Ciencia Penal y Criminología*, 25, 1-39. <http://criminnet.ugr.es/recpc/25/recpc25-29.pdf>
- Zaffaroni, E. R. (2006). *El enemigo en el derecho penal*. Ediar.
- Zaffaroni, E. R., Alagia, A. y Slokar, A. (2002). *Derecho penal. Parte general*. Ediar.