Revista Debate Jurídico Ecuador. Revista Digital de Ciencias Jurídicas. UNIANDES
ISSN 2600-5549/ Vol. 9 / Nro. 3 / septiembre- diciembre / Año. 2026 / pp. 482-495

ARTÍCULO DE REVISIÓN

MARCO JURÍDICO DE CIBERDELITOS Y PROTECCIÓN DE MENORES EN PERÚ, ECUADOR Y REINO UNIDO

LEGAL FRAMEWORK FOR CYBERCRIME AND CHILD PROTECTION IN PERU, ECUADOR, AND THE UNITED KINGDOM

Linares Otiniano, Ghyordano Martín
2025130040@unheval.pe
Universidad Nacional Hermilio Valdizán, Huánuco, Huánuco, Perú
https://orcid.org/0009-0008-1264-0511

García Ponce, Sara Herminia
shgarciap@epgunheval.edu.pe
Universidad Nacional Hermilio Valdizán, Huánuco, Huánuco, Perú
https://orcid.org/0009-0004-8900-5496

Pairazamán Silva, Victoria Consuelo
vpairazaman@gmail.com
Universidad Nacional Hermilio Valdizán, Huánuco, Huánuco, Perú
https://orcid.org/0009-0003-1536-0578

Recibido: 17/02/2026
Revisado: 19/02/2026
Aprobado: 28/07/2026
Publicado: 01/09/2026

DOI: https://doi.org/10.61154/dje.v9i3.4750

RESUMEN

La investigación aborda la insuficiencia del marco jurídico frente a los ciberdelitos contra menores en Perú y Ecuador, frente al creciente uso de tecnologías por niños, niñas y adolescentes. Mediante un enfoque cualitativo, documental y comparativo, se analizó la normativa vigente, la práctica institucional y casos recientes, entre ellos la operación “Gran Fénix 7- Pandora 1” y sentencias por grooming para identificar vacíos normativos y fallas procesales. Los hallazgos muestran que, pese a la tipificación de conductas como grooming y pornografía infantil, existen deficiencias en prevención, escasa responsabilidad legal de plataformas, ausencia de reglas claras sobre consentimiento digital y limitaciones probatorias que obstaculizan la persecución penal. La comparación con el marco del Reino Unido con instrumentos con Online Safety Act 2023 y la *Sexual Offences* Act 2003, evidencia medidas preventivas, deberes de las plataformas, verificación de edad y sanciones efectivas que

podrían guiar reformas. Se establece que la solución requiere reformas normativas focalizadas, mayor responsabilidad tecnológica, fortalecimiento institucional, educación digital y cooperación internacional para velar por una seguridad integral de los menores en el ciberespacio.

DESCRIPTORES DE CONTENIDO: Protección de datos; delito informático; cibercrimen; Derecho de la informática; Derecho del ciberespacio.

ABSTRACT

The research addresses the inadequacy of the legal framework for cybercrimes against minors in Peru and Ecuador, given the growing use of technology by children and adolescents. Using a qualitative, documentary, and comparative approach, the study analyzed current regulations, institutional practices, and recent cases, including Operation Gran Fénix 7-Pandora 1 and grooming convictions, to identify regulatory gaps and procedural flaws. The findings show that, despite the criminalization of behaviors such as grooming and child pornography, there are deficiencies in prevention, limited legal responsibility of platforms, a lack of clear rules on digital consent, and evidentiary limitations that hinder criminal prosecution. A comparison with the UK framework, with instruments such as the Online Safety Act 2023 and the Sexual Offences Act 2003, highlights preventive measures, platform responsibilities, age verification, and effective sanctions that could guide reforms. It is established that the solution requires targeted regulatory reforms, greater technological responsibility, institutional strengthening, digital education, and international cooperation to ensure comprehensive protection of minors in cyberspace.

CONTENT DESCRIPTORS: *Data protection; computer crime; cybercrime; Information technology law; Cyberspace law.*

INTRODUCCIÓN

Desde el siglo XX el desarrollo acelerado de las tecnologías de la información y comunicación, junto con la creciente dependencia de internet, ha modificado significativamente las dinámicas sociales, económicas y culturales de la sociedad contemporánea se han transformado profundamente. Sin embargo, este avance también ha significado la aparición de nuevas formas de criminalidad en el entorno digital, entra las cuales los más propensos a ser las víctimas de esos delitos son los niños, niñas y adolescentes, quienes constituyen uno de los grupos más vulnerables frente a los riesgos del ciberespacio (Trejos & Peláez, 2023).

Los factores imperantes para que se den los ciberdelitos en jóvenes y niños es principalmente el poco o en algunos casos el inexistente control para que los menores naveguen en el

internet, y esa responsabilidad de control recae en los apoderados (Peñuela, 2023; Quesada et al., 2022). Fenómenos como el grooming, el acoso digital, la difusión de contenido ilícito constituyen conductas delictivas de alta repercusión, cuyas consecuencias pueden derivar en hechos aún más graves como el secuestro o el suicidio. En este sentido, tales situaciones evidencian la complejidad de estas conductas y el hecho de establecer respuestas jurídicas eficaces (Jeglic et al., 2023).

El problema de los delitos informáticos contra menores no afecta únicamente a un país de manera aislada; constituye, más bien, un fenómeno de alcance global. En este contexto, el presente artículo examina los casos de Perú y Ecuador, tomando como referencia el modelo jurídico desarrollado por el Reino Unido en materia de regulación del ciberespacio, el cual busca suplir las lagunas y vacíos normativos existentes en ese ámbito. Asimismo, resulta evidente que los riesgos presentes en el ciberespacio ecuatoriano no solo comprometen la información y la reputación de las personas afectadas, mediante la sustracción de fotografías personales o el acceso ilícito a cuentas digitales; además ponen en peligro la seguridad de las infraestructuras de las entidades públicas (Cedeño, 2022).

La problemática de la suplantación de identidad en plataformas digitales en el contexto peruano constituye una creciente preocupación, al tratarse de un fenómeno que ha encontrado en el avance de las tecnologías un medio propicio para su expansión. Este ciberdelito, caracterizado por la usurpación de la identidad de una persona en el entorno digital compromete gravemente al prestigio, el honor y en numerosos casos, el patrimonio económico de las víctimas (Azcona et al., 2025).

Por ello el tomar de referencia legislaciones más consolidadas permite realizar un análisis crítico elemental. En este contexto diversos estudios señalan que el Reglamento General de Protección de Datos de la Unión Europea es uno de los modelos más robustos en materia de resguardo de datos personales (Fanni, 2024). No obstante, aunque este modelo constituye un referente general en protección de datos, no regula de forma específica la prevención de ciberdelitos contra menores. Por ello, el estudio también considera el marco normativo del Reino Unido, que incorpora regulaciones más especializadas en seguridad digital infantil y responsabilidad de los proveedores de servicios en línea, constituyendo el principal modelo de referencia para el análisis comparativo.

En el contexto peruano, si bien se han implementado diversas normas orientadas a regular lo delitos informáticos y proteger a los menores de edad, normas como la ley No 30096- Ley de los Delitos Informáticos (Ministerio Público Fiscalía de la Nación, 2024). el Decreto Legislativo 1410 (Ministerio de la Mujer y Poblaciones Vulnerables de Perú, 2018) y en Ecuador el Código Orgánico Integral Penal reformado en el año 2021 (Asamblea Nacional de la República del

cc BY NC SA

Ecuador, 2021) a pesar de ello, persisten limitaciones en el marco jurídico que dificultan una protección integral frente a estas conductas.

Estas deficiencias se ven plasmadas en los vacíos normativos. El archivamiento de numerosos casos se explica, en gran medida, por la falta de identificación de los presuntos responsables en la etapa de diligencias preliminares. Esta dificultad investigativa reduce la efectividad del sistema jurídico y afecta la capacidad del ordenamiento legal para garantizar seguridad en el espacio digital (Salvador, 2024; Velázquez, 2025).

El porqué de esta investigación es examinar la insuficiencia del marco jurídico peruano frente a los delitos informáticos contra menores de edad, evaluando sus principales limitaciones y contestándolos con modelos normativos de otros países, particularmente aquellos que han desarrollado regulaciones más consolidadas en la materia. A través de un enfoque comparativo con legislaciones como la de Ecuador, se busca identificar fortalezas, debilidades y posibles mejoras aplicables. Asimismo, busca contribuir al debate jurídico sobre la necesidad de fortalecer la regulación y las políticas públicas orientadas a la protección de menores en el entorno digital, promoviendo un sistema legal más eficaz que responda a los desafíos actuales de la criminalidad informática.

MÉTODOS

La presente investigación se desarrolló bajo un enfoque cualitativo, orientado al análisis jurídico de las falencias existentes en el marco normativo sobre ciberseguridad que afectan niños, niñas y adolescentes en entornos digitales. Este enfoque permitió identificar vacíos normativos y limitaciones en la protección jurídica de los menores frente a nuevas formas de criminalidad informática.

El estudio adoptó un diseño documental y comparativo, basado en el análisis de normas jurídicas, doctrina especializada, informes institucionales y estudios previos relacionados con la protección de menores en el entorno digital. En particular se analizó la legislación vigente en Perú y Ecuador en materia de delitos informáticos y protección de datos personales, contrastándola con el modelo regulatorio desarrollado por Reino Unido, considerado un referente internacional en la regulación del ciberespacio.

Asimismo, la investigación tuvo un alcance descriptico y analítico, al caracterizar las principales disposiciones normativas de los países estudiados, identificar sus similitudes y diferencias, y evaluar su efectividad en la prevención y sanción de los delitos informáticos contra menores. A partir de este análisis comparado, se examinaron los elementos del modelo

británico aplicables al contexto peruano y ecuatoriano con la finalidad de fortalecer la protección jurídica y reducir los riesgos en el entorno digital.

Como técnica de investigación se emplearon el análisis documental de legislación nacional e internacional y el análisis de contenido, lo que permitió interpretar la información recopilada, identificar patrones normativos y proponer mejoras en los ordenamientos jurídicos analizados.

RESULTADOS

En la actualidad, si bien los avances en las tecnologías informáticas han generado importantes innovaciones y automatizaciones que facilitan la vida cotidiana, también han traído consigo nuevas problemáticas sociales. Entre ellas algunos autores advierten la aparición de una forma de “dependencia tecnológica” vinculada al uso excesivo de dispositivos electrónicos como los teléfonos celulares, cuyo impacto resulta especialmente alarmante en niños, niñas y adolescentes.

Esta realidad evidencia que el acceso a dispositivos electrónicos no distingue edades, pues los menores desde etapas muy tempranas utilizan frecuentemente estos medios, muchas veces en reemplazo del acompañamiento y cuidado que corresponde a los padres. En numerosos casos, el uso de pantalla se convierte en un mecanismo inmediato para calmar el llanto, el enojo o el aburrimiento, pese a que los niños, niñas y adolescentes aún no cuentan con la madurez neurológica ni emocional suficiente para un uso responsable de dichas tecnologías.

Estas situaciones incrementan su vulnerabilidad frente a diversas modalidades de ciberdelincuencia, tales como el acoso sexual en línea, el grooming, el ciberbullying, la difusión o tráfico de imágenes de menores e incluso conductas que pueden derivar en consecuencias graves como el secuestro o el suicidio, fenómenos que evidencia un incremento progresivo.

Según los datos estadísticos en Ecuador más del 90% de la población dispone de teléfonos celulares con acceso a redes sociales, además dentro de dicha población encontramos a niños desde los cinco años. El sector que más usa estás tecnologías son los adolescentes y adultos. Por ello, este alto índice ejemplifica la enorme importancia y lo urgencia de fortalecer los mecanismos de regulación y protección frente a los ataques cibernéticos, sobre todo cuando pueda implicar a menores (Toledo & Ochoa, 2021).

Un ejemplo de la presencia de estos ciberdelitos es lo ocurrido el 13 de febrero de 2025, la Policía Nacional de Ecuador llevó a cabo el operativo denominado “Gran Fénix 7- Pandora 1” en las ciudades de Quito y Esmeralda, bajo la dirección de la fiscalía general del Estado. Como resultado de esta intervención se logró desarticular una organización criminal dedicada

a la producción y difusión de material de abuso sexual infantil, procediéndose a la aprehensión de cuatro personas. La investigación realizada mediante cooperación entre autoridades ecuatorianas y estadounidenses permitió identificar una red que producía y comercializaba actos en contra de la integridad sexual infantil. El contenido era vendido a ciudadanos extranjeros mediante videollamadas y plataformas de mensajería digital, generando ganancias a través de transferencias internacionales (Policía Nacional del Ecuador, 2025)

El caso evidencia la creciente complejidad de las organizaciones criminales en el entorno digital y la magnitud de los riesgos a los que se encuentran expuestos los menores en el ciberespacio. A su vez, pone en manifiesto la necesidad de fortalecer los mecanismos jurídicos y las estrategias institucionales contra niños, niñas y adolescente.

En Perú, la fiscalía provincial en Ciberdelincuencia de La Libertad obtuvo sentencia contra un sujeto debido a el delito de insinuaciones con fines sexuales a población infantil y adolescentes a través de aplicativos en línea (*Child Groomig*), en agravio de un menor de 11 años de edad. Según la investigación fiscal, el padre de la víctima denunció haber descubierto conversaciones de contenido sexual entre su hijo y un usuario de la red social Instagram, quien solicitaba fotos y videos íntimos al menor y lo manipuló para concretar un encuentro presencial en las inmediaciones de su domicilio (Ministerio Público Fiscalía de la Nación, 2025).

Es alarmante como el uso de plataformas digitales facilita la comisión de delitos sexuales contra menores de edad, aprovechando su vulnerabilidad y la facilidad de interacción en entornos virtuales. Es, por tanto, que ello pone en manifiesto los riesgos asociados al acceso temprano y no supervisado a redes sociales, así como el estar más alertas en la prevención, detección y sanción frente a estas conductas delictivas. En ese sentido, la intervención de las autoridades refleja la importancia de una respuesta institucional efectiva, pero también evidencia los desafíos que enfrenta el sistema jurídico peruano para garantizar una protección integral de los derechos de niños, niñas y adolescentes en el entorno digital.

Otro caso registrado en el Perú evidencia los riesgos del entorno digital para los menores. Un niño de nueve años intento ser captado por un joven de veinte años de edad a través del videojuego *Free Fire*. Según las investigaciones, el sujeto utilizaba la modalidad de grooming para obtener material íntimo de niños, niñas y adolescentes conectados a través de internet. La intervención se realizó tras la denuncia de la familia de la víctima y comprendió la incautación de equipos tecnológicos para el análisis forense correspondiente. En el cuadro 1 se hace una comparación entre Perú, Ecuador y el Reino Unido.

Cuadro 1. Comparación entre Perú, Ecuador y el Reino Unido.

Aspecto	Perú	Ecuador	Reino Unido
Normativa principal	Ley N.°30096(Delitos informáticos) – Ley N°. 29733(Protección de Datos Personales).	Código orgánico Integral Penal- Ley Orgánica de Protección de Datos Personales (2021).	Online Safety Act (2023) y Sexual Offences Act (2003).
Protección de datos de menores	La ley protege datos personales de forma general sin establecer un régimen diferenciado o reforzado para menores de edad, lo que limita su protección en entornos digitales.	Reconoce el tratamiento de datos personales y contempla la protección del menor como sujeto vulnerable, estableciendo mayor control sobre el uso de su información.	Protección reforzada de datos infantiles, con obligaciones estrictas para empresas que procesan información de menores y control del uso de sus datos en servicios digitales
Delitos informáticos contra menores	Se sancionan conductas como pornografía infantil y propuestas sexuales a menores por medios digitales(grooming), pero la regulación es limitada y no cubre integralmente todos los riesgos digitales actuales.	Tipifica de manera más amplia delitos de explotación sexual digital y conductas ilícitas en línea contra menores, ofreciendo mayor cobertura penal.	Regulación amplia del grooming, explotación sexual infantil online, posesión y distribución de material ilegal y preparación para abuso, con sanciones severas y persecución activa del delito.
Consentimiento digital del menor	No existe regulación clara o condiciones específicas para el consentimiento del menor en servicios digitales, generando vacíos jurídicos.	Reconoce el consentimiento como requisito para el tratamiento de datos personales e incorpora reglas más claras sobre su aplicación en menores.	Exige verificación de edad y mecanismos de consentimiento parental para el acceso de menores a servicios digitales, priorizando su seguridad.

Medidas preventivas de protección	El sistema se centra principalmente en sancionar delitos una vez cometidos, con escasas políticas preventivas especializadas en riesgos digitales que afecten a menores.	Ha desarrollado progresivamente políticas y mecanismos de prevención frente a riesgos digitales y protección de grupo vulnerables.	Sistema preventivo fuerte que obliga a plataformas a evaluar riesgos, eliminar contenidos dañinos y evitar contacto peligroso con menores antes de que ocurra el delito.
Nivel general de protección jurídica del menor	Protección jurídica limitada, con regulación general y ausencia de enfoque especializado en protección digital infantil.	Protección intermedia con avances en regulación penal y protección de datos personales	Alto nivel de protección jurídica con regulación específica, enfoque preventivo y responsabilidad tecnológica obligatoria.

Exposición de los hallazgos

Los ciberdelitos contra niños, niñas y adolescentes han adquirido mayor relevancia en el entorno digital, evidenciando nuevas formas de criminalidad que afectan su seguridad e integridad. Los casos analizados en Ecuador y Perú muestran que plataformas digitales, redes sociales y videojuegos facilitan delitos como el grooming y la explotación sexual infantil, lo que evidencia limitaciones en los mecanismos de prevención y protección jurídica. Ante estas limitaciones normativas, se identifican modelos regulatorios más desarrollados, como el del Reino Unido, que cuenta con marcos legales específicos orientados a la protección de los menores en entornos digitales, entre ellos la (Online Sfety Act , 2023), que establece obligaciones para las plataformas digitales en la prevención de contenidos perjudiciales para menores y la *Sexual Offences Act* 2003 que tipifica conductas como el grooming y otros delitos sexuales contra menores en línea. Estas normativas constituyen referencias relevantes para identificar vacíos en la legislación de Perú y Ecuador y proponer el fortalecimiento de sus marcos jurídicos en materia de prevención, protección digital y responsabilidad de los proveedores de servicio de internet.

En ese sentido, el análisis de casos concretos en Ecuador y Perú permite evidenciar los vacíos normativos existentes en la protección de menores en entornos digitales, los cuales justifican la necesidad de fortalecer sus marcos jurídicos.

En Ecuador, con el acontecimiento que se dio en las ciudades de Quito y Esmeraldas, donde se ejecutó el operativo “Gran Fénix 7- Pandora 1”, bajo la dirección de la Fiscalía. Donde se encontró una organización criminal dedicada a la producción y comercialización de material de abuso sexual infantil. Este caso demuestra la dimensión transnacional de estos delitos y la necesidad de fortalecer la cooperación internacional y los mecanismos preventivos.

En el Perú, la Fiscalía provincial en Ciberdelincuencia obtuvo sentencia contra un individuo por grooming en agravio de un menor de once años, a quien contactó por Instagram con fines sexuales. Ello muestra la vulnerabilidad de los menores en las redes sociales y la necesidad de reforzar las políticas de prevención y control del uso de estas plataformas.

Asimismo, la Policía Nacional del Perú intervino a un joven en Lurín acusado de captar a un menor de nueve años mediante el videojuego *Free Fire* para obtener material íntimo. Este hecho demuestra que los entornos digitales interactivos también pueden ser utilizados para la manipulación de menores, lo que exige mayores mecanismos de supervisión y regulación

En conjunto, estos casos evidencias que tanto Ecuador como Perú priorizan la persecución penal posterior al delito, sin desarrollar suficientemente estrategias preventivas ni mecanismos especializados de protección digital infantil, lo que revela la necesidad de fortalecer sus marcos normativos e institucionales

DISCUSIÓN

Los estudios recientes sobre la regulación de los ciberdelitos evidencian importantes desafíos en la capacidad de los Estados para garantizar una protección jurídica eficaz frente a los riesgos que enfrentan los menores de edad en el ciberespacio. La naturaleza internacional de los delitos informáticos, el anonimato y la rápida evolución tecnológica dificultan su investigación, persecución y sanción, lo que revela limitaciones en los marcos normativos vigentes. En Ecuador Ordóñez (2024) señala que la Ley Orgánica de Protección de Datos Personales, promulgada en 2021, constituye un avance en materia de regulación digital; sin embargo, diversos estudios sostienen que su aplicación aún resulta limitada en la prevención efectiva de los ataques cibernéticos. Como también se advierte en la ausencia de normas especializadas que regulen de manera integral el uso de tecnologías emergentes como la inteligencia artificial, lo que genera vacíos jurídicos que pueden ser aprovechados para la comisión de ciberdelitos. La falta de regulación específica en estos ámbitos refleja la necesidad de fortalecer el marco legal para prevenir riesgos digitales y proteger de manera efectiva a los menores de edad.

Con Perú se da algo parecido Alcalá (2025) menciona que el ciberespacio carece de fronteras claras y presenta serias dificultades regulatorias, lo que otorga ventaja al cibercriminal debido

al anonimato, el embrollo tecnológico, la insuficiencia de mecanismos probatorios y las deficiencias de la normativa procesal respecto a la prueba digital.

Sin embargo, al comparar estos vacíos normativos con el marco jurídico de Reino Unido, se observa la existencia de regulaciones más específicas orientadas a la protección de menores en entornos digitales. La legislación británica incorpora mecanismos especializados de control de contenidos en línea y la clara clasificación jurídica de los delitos sexuales perpetrados contra menores mediante el uso de tecnologías, lo que contribuye a reforzar las acciones orientadas a su identificación.

Este enfoque normativo evidencia un mayor desarrollo en la seguridad digital infantil al establecer obligaciones concretas para plataformas digitales y mecanismos de supervisión más estrictos frente a los riesgos del ciberespacio. En ese sentido, el modelo del Reino Unido constituye una referencia relevante para fortalecer los marcos jurídicos de Perú y Ecuador, especialmente en la regulación de servicios en línea, la protección reforzada de menores y la responsabilidad de los intermediarios digitales.

El impacto de la regulación jurídica frente a los ciberdelitos contra menores de edad, resulta cada vez más relevante en los ordenamientos jurídicos de Perú y Ecuador, donde la normativa si bien ha tratado de ajustarse a las legislaciones internacionales contra ciberdelitos aún presenta limitaciones para asegurar un resguardo contra el grupo más vulnerables que son los menores en entornos virtuales. Es así que Ecuador se adhirió recientemente hace unos años al convenio de Budapest, cuyo convenio también es importante para el control y regulación de ciberdelitos.

En este contexto, la existencia de vacíos normativos, la limitada regulación específica sobre ciberdelitos contra menores y la falta de mecanismos especializados para prevenir y sancionar conductas como el grooming o la explotación sexual en línea reducen la eficacia de la respuesta jurídica contra estas nuevas formas de criminalidad informática.

En este sentido, el marco normativo del Reino Unido constituye un referente relevante, debido a que incorpora regulaciones específicas orientadas a la seguridad digital infantil y a la responsabilidad de las empresas en línea. Entre estas destaca la *Online Safety Act* (2023), que establece el deber legal de las plataformas digitales de prevenir y eliminar contenidos perjudiciales para menores de edad, imponiendo mecanismos de verificación de edad y sanciones a las empresas que incumplan dichas obligaciones. Asimismo, normas como la *Sexual Offences Act* (2003) tipifican conductas como el grooming y otros delitos sexuales cometidos mediante medios digitales, mientras que la *Protection of Children Act* (1978)

sanciona la producción, posesión y distribución de material de explotación sexual infantil, incluso en entornos virtuales. Estas disposiciones evidencian un modelo regulatorio integral que combina medidas preventivas, sancionadoras y de responsabilidad tecnológica, configurando un sistema más especializado en comparación con los marcos normativos de países latinoamericanos como Perú y Ecuador.

A pesar de las reformas normativas implementadas en Perú y Ecuador respecto a los ciberdelitos contra menores, el estudio identifica persistentes deficiencias en su eficacia principalmente relacionadas con la falta de implementación efectiva de las normas existentes y la ausencia de regulaciones claras y especializadas en determinados ámbitos de protección digital infantil. Asimismo, se evidencia una limitada educación en materia de protección de datos y prevención de riesgos en el entorno digital, tanto a nivel social como familiar lo que se refleja en la falta de supervisión por parte de los apoderados en las actividades de los menores en internet, como las interacciones en redes, chats o videojuegos en línea.

Por lo tanto, la perspectiva futura requiere que ambos países fortalezcan sus marcos jurídicos y se alineen con modelos normativos más desarrollados en materia de protección digital infantil. En particular, el marco legislativo del Reino Unido constituye un referente relevante, debido a sus mecanismos más estrictos de regulación, control y responsabilidad en la protección de menores en entornos digitales, lo que permitiría garantizar mayor seguridad y control sobre los datos personales de niños, niñas y adolescentes.

No obstante, de los principales desafíos es la aplicación poco rigurosa de sanciones frente a los ciberdelitos. A diferencia de otros modelos normativos más estrictos, la falta de medidas sancionadoras severas reduce la eficacia de la protección jurídica.

Pese a estas limitantes, los estudios sugieren que los sistemas de protección pueden fortalecerse progresivamente mediante una mayor participación de las familias en la supervisión digital de los menores, el desarrollo de políticas educativas de prevención, el fortalecimiento institucional y la adopción de medidas legislativas más rigurosas orientadas a la prevención y sanción de los ciberdelitos**.**

CONCLUSIONES

El análisis realizado permite concluir que el marco jurídico vigente en Perú resulta aún insuficiente para enfrentar de manera integral los delitos informáticos contra menores de edad en el entorno digital. Si bien existen normas orientadas a sancionar accionares como el grooming, la explotación sexual en línea y otros ciberdelitos, estas presentan limitaciones en su aplicación, alcance preventivo y especialización en la protección digital infantil, lo que reduce la eficacia del sistema de protección jurídica.

cc BY NC SA

El estudio comparativo evidencia que en Ecuador se han desarrollado avances en materia de regulación digital y protección de datos personales; sin embargo, al igual que en el caso peruano, persisten vacíos normativos, dificultades en la implementación efectiva de las normas y limitaciones en los mecanismos de prevención y control de los riesgos que enfrentan los menores en el ciberespacio. Los casos analizados en ambos países demuestran que las legislaciones actuales priorizan la sanción posterior al delito, sin consolidar políticas preventivas especializadas ni sistemas de protección digital reforzada.

En contraste, el modelo regulatorio del Reino Unido evidencia un mayor desarrollo normativo en la protección de menores en entornos digitales, al incorporar medidas preventivas, obligaciones específicas para las empresas que ofrecen servicios mediante el uso del internet, mecanismos de control de contenidos y sanciones más estrictas frente a conductas delictivas. Este enfoque integral constituye un referente relevante para el fortalecimiento de los marcos jurídicos latinoamericanos, particularmente en la regulación de plataformas digitales, la verificación de edad y la responsabilidad tecnológica, de igual forma, la investigación confirma que la protección efectiva de los menores frente a los ciberdelitos no depende únicamente del fortalecimiento normativo, también de su correcta aplicación, la educación digital, las políticas de prevención, el fortalecimiento institucional y la supervisión familiar del uso de la tecnología. Por ello, es necesario promover reformas que incorporen mecanismos preventivos, refuercen la responsabilidad de las plataformas digitales y establezcan sistemas jurídicos más eficaces para precautelar la seguridad e integridad de los menores en el entorno digital.

REFERENCIAS

Alcalá, F. (2025). Cibercriminalidad: retos y desafíos para la administración de justicia peruana. *Poder Judicial*, 17(23), 205-248. https://revistas.pj.gob.pe/revista/index.php/ropj/article/view/906/1606

Asamblea Nacional de la República del Ecuador. (2021). *Código Orgánico Integral Penal Reformado (COIP).* https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Azcona, G., Alama, A.A., Gonzales, P.A., Ore, A., & Medrano, A.C. (2025). Abordaje, desafíos y evolución de la legislación sobre suplantación de identidad degital en Perú. *Revista Sapientia & Iustitia*, (12), 5-36. https://sapientia.ucss.edu.pe/index.php/sei/article/view/155/105

Cedeño, R. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual de Ecuador. *Revista Tecnológica Ciencia y Educación Edwards Deming*, 50-62. https://revista-edwardsdeming.com/index.php/es/article/view/88/158

Fanni, S. (2024). El reglamento general de protección de datos ante los desafíos tecnológicos: la arquitectura de la responsabilidad y de la indemnización del daño inmaterial en caso de ciberataque. *Revista de Privacidad y Derecho Digital*, *9*(35), 151-204. https://revista.proeditio.com/rpdd/article/view/7887

Jeglic, E. L., Winters, G. M., & Johnson, B. N. (2023). Identification of red flag child sexual grooming behaviors. *Child Abuse & Neglect*, *136*, 105998. https://www.sciencedirect.com/science/article/pii/S0145213422005324

Legislation.gov.uk (2023). *Online Safety Act 2023*. *is up to date with all changes known to be in force on or before 17 August de 2025.* https://www.legislation.gov.uk/ukpga/2023/50/contents

Ministerio de la Mujer y Poblaciones Vulnerables de Perú. (2018). *Decreto Legislativo 1410.* https://www.gob.pe/institucion/mimp/noticias/18866-gobierno-publica-decreto-legislativo-que-incorpora-acoso-y-chantaje-sexual-al-codigo-penal

Ministerio Público Fiscalía de la Nación de Perú. (2024). *Ley N°30096. Ley de Delitos Informáticos.* https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

Ministerio Público Fiscalía de la Nación. (2025). *Fiscalía Especializada en Ciberdelincuencia obtiene sentencia contra sujeto que contactó a menor de edad para pedirle fotos y videos íntimos.* https://l1nq.com/d1wxqqm

Ordoñez, L. A. (2024). El marco legal de los delitos cibernéticos en Ecuador. *Reincisol.*, *3*(5), 1447-1469. https://www.reincisol.com/ojs/index.php/reincisol/article/view/158

Peñuela, L. C. (2023). Ciberseguridad: el peligro al acecho de los niños, niñas y adolescentes. *Informática y Derecho: Revista Iberoamericana de Derecho Informático (segunda época)*, (13), 15-28. https://agora.edu.es/servlet/articulo?codigo=9265273

Policía Nacional del Ecuador. (2025). *Red de pornografía infantil es desarticulada en Quito y Esemraldas.* https://noticias.policia.gob.ec/red-de-pornografia-infantil-es-desarticulada-en-quito-y-esmeraldas/

Quezada, P., Suárez, E.A., Coloma, E.X., Ruiz, R.R., Pinos, B.P., Espinoza, E.P., Arrono, C.J., & Martínez, C.E.(2022). Sobreexposición de adolescentes a Ciberdelitos en el Ecuador. *Revista Ibérica de Sistema e Tecnologías de información*, E(54), 419-424. https://sl1nk.com/nhp68wq

Salvador, C. T. E. (2024). La impunidad en los delitos informáticos. Una problemática de poco interés por los legisladores, jueces y fiscales. *Ius vocatio*, *7*(9), 91-115. https://revistas.pj.gob.pe/revista/index.php/iusVocatio/article/view/928

Todelo, D., & Ochoa, F. (2021). Derechos fundamentales y criminalidad cibernética en niños,niñas y adolescentes: análisis para la no indefensión de la víctima. *FIPCAEC*, 6(4), 336-363. https://ftp.polodelconocimiento.com/index.php/fipcaec/article/view/485/847

Trejos, C. A., & Peláez, Y. (2023). Ciberdelitos en menores de edad en la red social Facebook: revisión sistemática de literatura. *Nuevo derecho*, *19*(32), 1-18. https://www.redalyc.org/journal/6697/669778487007/669778487007.pdf

Velázquez, M. E. (2025). "Ciberolvido legislativo" en el Perú: impactos problemáticos de las recientes modificaciones a la Ley contra el Crimen Organizado en la ciberdelincuencia a la luz de la Convención de Palermo. *Revista Peruana de Derecho Internacional*, (181), 117-148. https://revista.spdi.org.pe/RPDI/article/view/849

©2026 por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0) (https://creativecommons.org/licenses/by-nc-sa/4.0/).