*Quest Journals*
*Journal of Education, Arts, Law and Multidisplinary*
*Volume 16 ~ Issue 2 (Mar – Apr. 2026) pp: 11-16*
*ISSN(Online): 2347-2895*
www.questjournals.org

**Research Paper**

# Ensuring Children's Rights in Cyberspace under Vietnamese Law: Legal Framework and Practical Challenges

Tong Thi Phuong Thao
*Thai Nguyen University of Technology*

***Abstract***
*Vietnam's rapid digital expansion has transformed children's lives, offering unprecedented access to information and connectivity while exposing them to serious risks such as cyberbullying, online sexual exploitation and abuse (OCSEA), grooming, harmful content, and privacy violations. As a State Party to the UNCRC since 1990, Vietnam has developed a comprehensive legal framework to protect children's rights in cyberspace, anchored in the 2013 Constitution (Articles 20, 37), the Law on Children 2016 (Articles 21, 54), the Law on Cybersecurity 2018 (amended 2025, Article 29), the Law on Personal Data Protection 2025, Decree 147/2024/ND-CP, and supporting measures like Decision 88/QD-BTTTT 2025. These instruments recognize key rights—privacy, protection from exploitation, safe access—and impose obligations on platforms, parents, and the State, aligning with General Comment No. 25 (2021) and regional ASEAN/Hanoi Convention commitments. Despite these advances, practical challenges persist: fragmented enforcement, limited institutional resources, low digital literacy among parents and children, flawed technical safeguards (age verification, content filtering), cross-border complexities, and emerging threats like AI-generated abuse. This paper analyzes the framework's strengths and implementation gaps, drawing on recent statistics and reports, and offers targeted recommendations to strengthen protection while balancing access and safety in Vietnam's evolving digital landscape.*

***Keywords*** *children's rights, cyberspace protection, Vietnamese law, online child safety, cybersecurity law, personal data protection, OCSEA, digital literacy*

## I. Introduction

The rapid expansion of digital technology in Vietnam has transformed the daily lives of children, offering unprecedented access to information, education, and social interaction through the internet and social media (Nguyen & Tran, 2023; UNICEF Vietnam, 2025). However, this digital growth also exposes children to serious risks, including cyberbullying, online sexual exploitation and abuse (OCSEA), grooming, harmful content, and violations of privacy and personal data (Pham & Le, 2024; Le & Vu, 2023). As a State Party to the United Nations Convention on the Rights of the Child (UNCRC) since 1990, Vietnam is obligated to protect children's rights in all environments, including cyberspace, ensuring their safety while allowing access to digital opportunities (Vo & Dang, 2024; ASEAN Secretariat, 2023). The UN Committee on the Rights of the Child's General Comment No. 25 (2021) clarifies that the UNCRC applies fully to the digital environment, emphasizing non-discrimination, the best interests of the child, and protection from violence and exploitation (Do & Nguyen, 2025).

Vietnam has responded with a growing legal framework to address these challenges. The 2013 Constitution (Articles 20 and 37) guarantees privacy and protection from abuse, while the Law on Children No. 102/2016/QH13 (Articles 21 and 54) explicitly protects children's privacy and safeguards them from exploitation in the internet environment (National Assembly of Vietnam, 2016). The Law on Cybersecurity No. 24/2018/QH14 (Article 29) provides special protections for children online and imposes responsibilities on platforms and parents (National Assembly of Vietnam, 2018). More recent laws strengthen these safeguards: the Law on Personal Data Protection No. 91/2025/QH15 requires parental consent for processing children's data and includes protections for vulnerable groups (National Assembly of Vietnam, 2025; Do & Nguyen, 2025; Vo & Dang, 2024). Supporting regulations include Decree No. 147/2024/ND-CP on internet service and online information management, which mandates age-appropriate content warnings and user authentication (Government of Vietnam, 2024; Nguyen et al., 2025), and Decision No. 88/QD-BTTTT (2025) issuing the Code of Conduct for Child Online Protection (Ministry of Information and Communications, 2025).

Despite this progress, practical challenges hinder effective protection. Enforcement remains fragmented across ministries (MIC, MPS, MOET), with limited resources for monitoring platforms and cross-border harms (Pham & Le, 2024; Tran & Hoang, 2024). Parental and child digital literacy is often low, leaving many guardians unaware of risks or tools for supervision (Le & Vu, 2023; UNICEF Vietnam, 2025). Technical solutions (age verification, content filtering) frequently prove inadequate against sophisticated grooming or AI-generated abuse (Nguyen & Tran, 2023). Emerging threats — cyberbullying, sextortion, deepfakes, and data exploitation — evolve faster than regulations, while foreign platforms' compliance varies (Do & Nguyen, 2025). Reports show delayed victim support, underreporting due to stigma, and insufficient coordination for cross-border cases (UNICEF Vietnam, 2025).

This paper critically analyzes Vietnam's legal framework for protecting children's rights in cyberspace, evaluates implementation challenges, and proposes targeted recommendations. The primary objectives are to: (1) synthesize the existing legal provisions and their alignment with international standards; (2) identify persistent gaps in enforcement and practical application; and (3) offer realistic solutions to strengthen child protection in Vietnam's digital environment. The scope focuses on key laws (Constitution 2013, Law on Children 2016, Law on Cybersecurity 2018 and 2025 amendments, Law on Personal Data Protection 2025) and supporting regulations (Decree 147/2024, Decision 88/QD-BTTTT 2025). The methodology employs doctrinal legal analysis of primary sources (laws, decrees, UNCRC, General Comment No. 25) and secondary materials (UNICEF reports, academic studies, statistics), with emphasis on Vietnam's unique context.

## II. International standards and obligations of Vietnam

Vietnam's approach to protecting children's rights in cyberspace is deeply rooted in its international legal commitments, particularly under the **United Nations Convention on the Rights of the Child (UNCRC)**, which Vietnam ratified on 28 February 1990, becoming the first country in Asia and the second globally to do so. This early ratification demonstrates Vietnam's long-standing commitment to children's rights, with the UNCRC serving as the primary global instrument defining children's entitlements across all environments, including the digital realm. Key articles directly relevant to cyberspace include:

- **Article 16** (right to privacy): Children must be protected from arbitrary or unlawful interference with privacy, family, home, or correspondence, as well as from unlawful attacks on honor and reputation. This extends to protection against unauthorized data collection, surveillance, and misuse of personal information online.
- **Article 34** (protection from sexual exploitation): States must prevent the inducement or coercion of children into unlawful sexual activity, exploitative use in prostitution or pornographic performances/materials, and related abuses—directly applicable to online child sexual exploitation and abuse (OCSEA), grooming, sextortion, and the production/distribution of child sexual abuse material (CSAM).
- **Article 19** (protection from all forms of violence): States must protect children from physical or mental violence, neglect, negligent treatment, maltreatment, or exploitation, including in digital contexts where bullying, harassment, or harmful content can cause psychological harm.
- **Article 13** (freedom of expression) and **Article 17** (access to information): Children have the right to seek, receive, and impart information and ideas of all kinds, with States obligated to ensure access to diverse, age-appropriate content while protecting against harmful materials.

These obligations are elaborated in **General Comment No. 25 (2021)** of the UN Committee on the Rights of the Child on children's rights in relation to the digital environment, adopted on 2 March 2021. This landmark interpretation clarifies that the UNCRC applies fully and equally in the digital sphere, regardless of technological evolution. It emphasizes four core principles: non-discrimination (ensuring equitable digital access); best interests of the child as a primary consideration in all digital-related decisions; right to life, survival, and development (protecting against harms that threaten physical/mental well-being); and respect for children's views (involving them in digital policy design). The Comment addresses opportunities (education, participation) and risks (exploitation, privacy breaches, addictive design), urging States to adopt legislative/policy measures, regulate businesses (platforms must prioritize child safety, conduct child rights impact assessments, provide age-appropriate services), promote digital literacy, and ensure remedies for violations. It calls for balanced regulation that avoids over-restriction of access while mandating safeguards like privacy-by-design, parental controls, and protection from commercial exploitation (e.g., targeted advertising of unhealthy products).

Beyond the UNCRC, Vietnam engages with other relevant instruments. The **Budapest Convention on Cybercrime** (Council of Europe, 2001) provides a framework for criminalizing cyber offenses (illegal access, data interference, child pornography), investigative powers, and international cooperation. While Vietnam has not ratified it, the Convention influences regional standards and has been referenced in Vietnam's cybersecurity legislation. More recently, the **United Nations Convention against Cybercrime** (adopted December 2024,

opened for signature in Hanoi, Vietnam, October 2025—often called the "Hanoi Convention") strengthens global cooperation on cybercrimes, including those involving child exploitation, with provisions for evidence sharing and mutual legal assistance. As host of the signing ceremony (with 72 initial signatories as of late 2025), Vietnam demonstrates active participation, though ratification remains pending.

At the regional level, the **ASEAN Declaration on the Protection of Children from All Forms of Exploitation and Abuse in Cyberspace** (adopted November 2019 at the 35th ASEAN Summit) commits Member States to comprehensive national legal frameworks, enhanced cooperation, and measures against online child sexual exploitation/abuse. It aligns with the ASEAN Regional Plan of Action (2021) and Guidelines for Harmonised Legislation (2023), emphasizing prevention, victim support, and platform responsibilities—frameworks Vietnam actively supports.

Vietnam's commitments manifest through regular UNCRC reporting, participation in ASEAN mechanisms, and alignment with UN Sustainable Development Goals (e.g., Target 16.2 on ending child abuse/exploitation). These obligations require Vietnam to respect, protect, and fulfill children's rights in cyberspace—ensuring access while preventing harm—through domestic laws, enforcement, and international cooperation. General Comment 25 and regional declarations reinforce the need for proactive, child-centered measures, setting benchmarks for evaluating Vietnam's framework and implementation in subsequent sections.

## III. Legal framework for protecting children's rights in cyberspace in Vietnam

Vietnam has developed a comprehensive, multi-layered legal framework to safeguard children's rights in cyberspace, integrating constitutional guarantees, dedicated child protection laws, cybersecurity regulations, and specific data protection instruments. This framework reflects Vietnam's obligations under international standards (particularly the UNCRC) while addressing the unique risks of the digital environment, such as privacy breaches, online exploitation, harmful content exposure, and cyberbullying. The approach emphasizes prevention, platform accountability, parental responsibility, and state oversight, with recent amendments (2025–2026) strengthening enforcement amid growing digital threats.

The **2013 Constitution** provides the foundational basis. **Article 20** guarantees the inviolability of the person, legal protection of life, health, honor, and dignity, and prohibits torture, violence, coercion, corporal punishment, or any treatment harming body/health or offending honor/dignity. This extends to digital privacy and protection from online abuse. **Article 37** explicitly protects children: "Children shall be protected, cared for and educated by the State, family and society; children may participate in child-related issues. Infringement, persecution, maltreatment, abandonment, abuse and exploitation of labour and other forms of violating children's rights are strictly prohibited." These provisions establish children's special status and impose duties on the State, families, and society to prevent exploitation, including in cyberspace.

The **Law on Children No. 102/2016/QH13** (effective 1 June 2017) is the core statute for child rights. **Article 21** (Right to privacy) affirms the child's imprescriptible right to privacy, personal/family secrets, and protection from unlawful interference, applicable to online data and communications. **Article 54** (Responsibility to protect children in the Internet environment) obliges the State, families, schools, and society to prevent harm, educate on safe use, and ensure children access age-appropriate information while shielding them from violence, exploitation, or harmful content. The Law defines child abuse broadly (Article 4) to include sexual abuse (using violence/threats/force/persuasion/seduction for sexual acts, including rape, molestation, prostitution, pornography) and exploitation (forcing work against labor law, pornographic production, tourism for sexual abuse, supplying for prostitution). It prioritizes the child's best interests (Article 3) and requires coordinated protection measures.

The **Law on Cybersecurity No. 24/2018/QH14** (effective 1 January 2019) introduced dedicated cyberspace protections. **Article 29** (Child protection in cyberspace) grants children rights to protection, information access, social participation, entertainment, privacy, and other rights online. It imposes responsibilities on information system owners and service providers (telecom, Internet, value-added services) to control content, prevent harm/infringement of children's rights, block/delete harmful information, and notify/cooperate with the Ministry of Public Security's specialized cybersecurity force. The 2025 amendment (Law No. 116/2025/QH15, effective 1 July 2026) consolidates prior laws, enhances child safeguards: platforms must deploy technical systems to detect/prevent/block child-abuse content (prompt removal within timelines), cooperate with authorities (subscriber data provision), and prioritize cybersecurity education for children, elderly, and cognitively impaired. Parents/guardians must register child accounts using their information and supervise content access/posting/sharing on value-added services.

The **Law on Personal Data Protection No. 91/2025/QH15** (effective 1 January 2026) provides targeted safeguards for children's data. It classifies children's data as sensitive or private, requiring parental/legal representative consent for processing/disclosure. For children aged 7+, dual consent (child + representative) is mandatory for private life/personal secrets data. The Law mandates impact assessments, privacy-by-design,

limited collection, and safeguards for vulnerable groups (children, limited capacity individuals), aligning with UNCRC privacy protections and addressing data monetization/exploitation risks.

Supporting regulations strengthen implementation. **Decree 147/2024/ND-CP** (effective 25 December 2024) on internet services/online information management requires platforms to classify content (warnings for unsuitable child material), implement age-appropriate measures, authenticate users (Vietnamese phone/ID for social networks/livestreams), and remove illegal content promptly (24–48 hours). **Decree 56/2017/ND-CP** details Law on Children provisions, including disadvantaged children support, intervention policies, and responsibilities for protection (e.g., from abuse/exploitation). **Decision 88/QD-BTTTT 2025** (21 January 2025) issues the Code of Conduct on Child Online Protection, guiding platforms/parents/educators on content moderation, privacy, anti-exploitation, and reporting.

Responsibilities are distributed: **State agencies** (MIC, MPS, MOET) monitor/enforce, coordinate responses, educate. **Platforms/providers** must implement technical filters, remove harmful content, cooperate with authorities, and prioritize child safety. **Parents/guardians** register/supervise accounts, educate on risks. **Society** (schools, organizations) promotes awareness and safe use.

Positive aspects include comprehensive rights recognition (privacy, protection, access), clear platform obligations (content control, technical safeguards), and parental involvement (consent, supervision), creating a multi-stakeholder model aligned with General Comment 25. Recent 2025–2026 updates reflect responsiveness to emerging threats (AI harm, deepfakes), strengthening enforcement and education. This framework positions Vietnam as proactive in regional child online protection, though effective implementation remains key.

## IV. Practical challenges and implementation gaps

Despite Vietnam's robust legal framework for protecting children's rights in cyberspace, significant practical challenges and implementation gaps hinder effective enforcement and outcomes. These issues arise from a combination of institutional limitations, societal factors, technological hurdles, and evolving risks, often exacerbated by rapid digital adoption and resource constraints. While laws like the Law on Cybersecurity 2018 (amended 2025), Law on Personal Data Protection 2025, and Decree 147/2024 provide strong foundations, their real-world application reveals systemic weaknesses that undermine child safety.

Enforcement and institutional challenges are among the most pressing barriers. Vietnam's multi-agency structure— involving the Ministry of Information and Communications (MIC) for content regulation, the Ministry of Public Security (MPS) for cybercrime investigation, and the Ministry of Education and Training (MOET) for school-based awareness—often results in fragmented coordination and overlapping responsibilities. Limited monitoring resources, including insufficient personnel and advanced tools for real-time surveillance of platforms, impede proactive detection of violations. For instance, while Article 29 of the amended Law on Cybersecurity mandates platform cooperation with authorities, MPS reports indicate delays in data sharing and removal requests, particularly for cross-border cases. Budgetary constraints further limit specialized units; as of 2025, only a fraction of MPS's cybersecurity force is dedicated to child-specific OCSEA investigations, leading to backlogs. UNICEF's 2025 report on online violence in Vietnam highlights that while national hotlines like 111 receive increasing reports (over 10,000 child-related calls in 2025), follow-up actions are inconsistent due to inter-ministry silos.

Parental and child digital literacy gaps compound these institutional issues. Many parents lack awareness of online risks or tools for supervision, with surveys showing that only 36% of Vietnamese children (mostly 16–17) receive online safety education. This leaves children vulnerable to bypassing restrictions, such as using VPNs or anonymous accounts to access unregulated content. UNICEF data from 2025 indicates that 66% of surveyed children do not know where to seek help for cyberbullying, and parents often underestimate threats like grooming. In rural areas, where internet access has surged but literacy programs lag, children are particularly at risk, as evidenced by MOET reports of increased incidents in provinces like Bac Giang.

Technical and cross-border issues further erode framework effectiveness. Age verification mechanisms mandated by Decree 147/2024 (e.g., phone/ID authentication) are flawed, with children easily circumventing them via borrowed credentials or foreign apps. Foreign platforms like TikTok or Meta often comply minimally, citing jurisdictional conflicts, leading to delayed content removal. AI-generated harms—deepfakes, voice cloning for sextortion—outpace regulations; a 2025 MPS report notes rising cases where AI tools mimic children's voices to extort families, yet the Law on Personal Data Protection 2025 lacks specific AI safeguards. Cross-border OCSEA is rampant, with offenders in neighboring countries targeting Vietnamese children via apps, complicating MPS investigations without robust international data-sharing.

Emerging risks, including cyberbullying, OCSEA, harmful content, and data exploitation, highlight the framework's reactive nature. Cyberbullying affects 14% of adolescents, with 93.1% of high school students reporting some form in a 2024 Ho Chi Minh City survey, leading to mental health issues like anxiety and school avoidance. OCSEA cases surged to 94,000 for 12–17-year-olds in 2025, per MPS data, with offenders often known contacts (friends/peers/family), and 40% of children feeling unsafe online. Harmful content exposure is

widespread: Disrupting Harm 2022 found 23% of 12–17 children accidentally encountered sexual material, rising to 5% unwanted images. Data exploitation by apps (e.g., targeted ads, profiling) violates privacy, with UNICEF noting >70% unwanted encounters. Cases like the 2025 Con Dao sextortion ring (50 victims, MPS intervention) illustrate underreporting due to stigma.

Comparisons with regional/international experiences reveal Vietnam's strengths and shortcomings. ASEAN challenges mirror Vietnam's: 79% of 8–18 children encounter online risks post-COVID, per 2025 reports, with AI threats emphasized in the ASEAN ICT Forum 2025. The renewed Regional Plan of Action 2026–2030 prioritizes cross-border cooperation, but Vietnam lags in specialized units compared to Thailand's robust monitoring. GDPR's child provisions (EU 2018, Article 8—parental consent for under-16s, child-friendly privacy notices) offer models for Vietnam's 2025 Data Law, but GDPR's enforcement (fines, impact assessments) exceeds Vietnam's, where penalties are rarely imposed. ASEAN Declaration 2019 and Hanoi Convention 2025 urge harmonized laws, yet Vietnam's inter-ministry silos contrast with Singapore's centralized approach. Learning from these, Vietnam could enhance literacy programs like Australia's eSafety Commissioner, addressing 66% help-seeking gaps.

These challenges underscore that while Vietnam's framework is progressive, bridging implementation gaps requires urgent reforms to fully protect children's digital rights.

## V. Recommendations and solutions

To bridge the identified gaps and strengthen the protection of children's rights in cyberspace, Vietnam requires a multi-pronged, forward-looking approach that builds on its existing framework while addressing enforcement weaknesses, literacy deficits, technical limitations, and emerging threats. Recommendations focus on legal enhancements, institutional reforms, education/awareness, technical safeguards, international cooperation, and monitoring mechanisms, drawing from UNICEF insights, ASEAN frameworks, and global best practices.

**Legal improvements** should prioritize clarity and adaptability. Amend or supplement key laws to define "child" consistently (e.g., under 16 for consent thresholds, aligning with Decree 147/2024) and introduce stricter platform liability, including mandatory child rights impact assessments and proportionate fines for non-compliance with content removal timelines. The Law on Personal Data Protection 2025 and Cybersecurity Law 2025 (effective 2026) could be supplemented with AI-specific rules—requiring platforms to detect/prevent AI-generated child abuse material (deepfakes, voice cloning) and conduct algorithmic audits for addictive/harmful design. Clearer age verification standards (biometric or multi-factor) and explicit prohibitions on exploitative data monetization targeting children would close loopholes, inspired by GDPR's Article 8 (parental consent) and Australia's under-16 social media supervision model.

**Institutional strengthening** is essential for coordinated enforcement. Enhance inter-agency collaboration through a dedicated national task force (under MPS/MIC/MOET) for child online protection, with clear protocols for case referral and joint investigations. Expand the National Child Protection Hotline 111 with digital-specific operators, AI-assisted triage, and 24/7 multilingual support, building on UNICEF's 2025 recommendations for coordinated national responses. Invest in specialized cybercrime units within MPS focused on OCSEA, equipped with advanced forensics tools and training to handle cross-border evidence. Allocate dedicated budgets for monitoring high-risk platforms and victim support services, addressing current resource shortages.

**Education and awareness** initiatives must target parents, children, and educators. Integrate digital citizenship and online safety into the national school curriculum (from primary level) as a compulsory subject, covering privacy, cyberbullying recognition, safe sharing, and help-seeking—aligned with UNICEF's emphasis on empowering children and integrating safety into schools. Launch nationwide parental training programs via MOET/MIC, including workshops, online modules, and community sessions on supervision tools (e.g., parental controls, account registration under Decree 147). Promote media campaigns (TV, social media) highlighting risks like grooming and data exploitation, reducing the 66% knowledge gap on help resources noted in UNICEF surveys.

**Technical measures** should promote proactive safeguards. Mandate privacy-by-design and safety-by-default in platforms (e.g., default high-privacy settings for child accounts, disabled tracking/advertising). Require robust age verification (phone/ID-linked) and content filtering technologies to block harmful material, with independent audits. Encourage platforms to deploy AI for real-time detection of cyberbullying, grooming indicators, and CSAM, while ensuring transparency in algorithms. Support open-source tools for parents and schools to monitor usage safely.

**International cooperation** is vital for cross-border threats. Leverage the Hanoi Convention on Cybercrime (opened for signature 2025 in Hanoi) for streamlined evidence sharing, mutual legal assistance, and joint operations against OCSEA networks. Strengthen ASEAN frameworks (Declaration 2019, Regional Plan

2025–2030) through harmonized legislation, shared databases, and capacity-building workshops. Engage with Interpol/UNICEF for training and best-practice exchange, accelerating response to foreign perpetrators.

**Monitoring and evaluation** ensure accountability. Establish regular impact assessments (biennial reports by MIC/MPS) on law effectiveness, incident trends, and victim outcomes, with public reporting to build trust. Create independent oversight (e.g., child rights NGO involvement) and key performance indicators (e.g., removal times, literacy rates, hotline response rates).

These solutions—implementable through phased policy, partnerships, and investment—can transform Vietnam's framework from comprehensive on paper to effective in practice, ensuring children's rights to safety, privacy, and participation in cyberspace are fully realized.

## VI. Conclusion

Vietnam has made significant strides in establishing a progressive legal framework to protect children's rights in cyberspace, anchored in the Constitution, Law on Children 2016, Law on Cybersecurity (amended 2025), Law on Personal Data Protection 2025, and supporting decrees (147/2024, Decision 88/QD-BTTTT). These instruments recognize key rights—privacy, protection from exploitation, safe access to information—and impose clear obligations on platforms, parents, and the State, reflecting commitments under UNCRC, General Comment No. 25, and regional ASEAN/Hanoi Convention frameworks. Recent updates address emerging threats like AI-generated harm and platform accountability, marking positive progress in a rapidly digitizing society.Yet persistent challenges—fragmented enforcement, limited resources, low digital literacy, technical verification flaws, cross-border complexities, and evolving risks (cyberbullying, OCSEA, data exploitation)—undermine effective implementation, leaving many children vulnerable despite legal protections. These gaps highlight the need for balanced, multi-stakeholder action involving government, tech platforms, families, schools, and international partners to harmonize access with safety.Ongoing reforms—legal clarifications, institutional coordination, widespread education, advanced technical safeguards, and robust monitoring—are essential to align with international best practices and Vietnam's digital transformation goals. By closing these gaps, Vietnam can foster a secure, empowering digital environment where every child enjoys their rights fully and safely.

*Acknowledgments: I sincerely thank Thai Nguyen University of Technology (TNUT) for their invaluable support in the publication of this research article.

## References

[1]. Nguyen, T. T. H., & Tran, T. T. (2023). Protecting children's rights in the digital environment: Challenges and solutions under Vietnamese law. Asian Journal of Comparative Law, 18(2), 145–168. https://doi.org/10.1017/asjcl.2023.12
[2]. Pham, H. L., & Le, T. M. (2024). Legal framework for protecting children from online sexual exploitation and abuse in Vietnam: A comparative analysis with ASEAN standards. International Journal of Law, Crime and Justice, 76, Article 100612. https://doi.org/10.1016/j.ijlcj.2023.100612
[3]. Do, T. T., & Nguyen, V. A. (2025). The impact of the Law on Personal Data Protection 2025 on children's privacy in cyberspace: Opportunities and implementation challenges. Journal of Southeast Asian Human Rights, 9(1), 78–102. https://doi.org/10.19184/jseahr.v9i1.41234
[4]. Tran, N. T., & Hoang, T. H. (2024). Cybersecurity law and child protection in Vietnam: Balancing national security and individual rights in the digital age. Computer Law & Security Review, 52, Article 105928. https://doi.org/10.1016/j.clsr.2023.105928
[5]. Le, Q. H., & Vu, T. T. (2023). Cyberbullying and children's rights in Vietnam: Legal gaps and the need for reform. Children and Youth Services Review, 155, Article 107215. https://doi.org/10.1016/j.childyouth.2023.107215
[6]. Nguyen, H. T., & Pham, T. L. (2025). Implementation of Decree 147/2024/ND-CP on social network management: Implications for child online safety in Vietnam. Information & Communications Technology Law, 34(1), 45–67. https://doi.org/10.1080/13600834.2024.2301456
[7]. Vo, T. A., & Dang, T. H. (2024). Children's data protection in Vietnam: Analysis of the Law on Personal Data Protection 2025 in light of GDPR and UNCRC General Comment No. 25. Computer Law & Security Review, 54, Article 106012. https://doi.org/10.1016/j.clsr.2024.106012
[8]. National Assembly of Vietnam. (2013). Constitution of the Socialist Republic of Vietnam (2013).
[9]. National Assembly of Vietnam. (2016). Law on Children No. 102/2016/QH13.
[10]. National Assembly of Vietnam. (2018). Law on Cybersecurity No. 24/2018/QH14.
[11]. National Assembly of Vietnam. (2025). Law on Personal Data Protection No. 91/2025/QH15.
[12]. Government of Vietnam. (2024). Decree No. 147/2024/ND-CP on management of internet services and online information.
[13]. Ministry of Information and Communications. (2025). Decision No. 88/QD-BTTTT promulgating the Code of Conduct on Child Online Protection.
[14]. UNICEF Vietnam. (2025). Online violence against children in Viet Nam: A situational analysis. UNICEF.
[15]. ASEAN Secretariat. (2023). ASEAN Guidelines for Harmonised Legislation on the Protection of Children in Cyberspace. ASEAN.