International Journal of Innovative Research and Scientific Studies, 8(3) 2025, pages: 4057-4068

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Policy recommendations for enhancing children's personal data protection: A case study in Vietnam

Thai Thi Tuyet Dung[1], Nguyen Van Duong[2*]

[1]*University of Economics and Law, Vietnam National University Ho Chi Minh City, 84, Vietnam.*
[2]*Ho Chi Minh City University of Law, Ho Chi Minh City, 84, Vietnam.*

Corresponding author: Nguyen Van Duong (*Email: nvduonglaw@gmail.com*)

Abstract

In the digital age, protecting children's personal data is an urgent global problem, especially in Vietnam, where children use the internet at an alarming rate. Therefore, the objective of this study is to measure the impact of crucial elements on children's personal data protection in Vietnam using structural equation modeling (SEM). The authors made concrete policy proposals to help lawmakers improve children's personal data protection. The methodology employed a structural equation model based on data collected through qualitative interviews with ten legal experts specializing in child rights protection. These specialists provide professional perspectives on the current legal framework, policy enforcement issues, and prospective reforms. Additionally, the quantitative approach is based on a study of 450 respondents in Ho Chi Minh City, Vietnam. The findings of the study revealed that five important variables have a favorable impact on children's personal data protection: the legal system (LS), coordination among agencies (CA), awareness and training (AT), technology development (TD), and monitoring and violation handling (MV). Finally, the practical consequences presented policy recommendations to assist managers and legislators in establishing a personal data protection commission, harmonizing scattered legislation into a dedicated personal data protection act, and increasing penalties in line with global standards.

Keywords: Awareness and training, Children's data protection, Digital transformation, Legal system.

DOI: 10.53894/ijirss.v8i3.7443
Funding: This research is funded by University of Economics and Law, National University Ho Chi Minh City, Vietnam.
History: Received: 4 April 2025 / **Revised:** 7 May 2025 / **Accepted:** 9 May 2025 / **Published:** 28 May 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: Both authors contributed equally to the conception and design of the study. Both authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Acknowledgments: The authors thank lecturers, managers, and rector of University of Economics and Law, National University Ho Chi Minh City, Vietnam.
Publisher: Innovative Research Publishing

1. Introduction

In a digital environment, protecting children's personal data is essential for their rights, privacy, and security. Thanks to internet platforms, social media, and instructional technologies, kids are more vulnerable to data tracking, cyber threats, and privacy abuses than ever. We can understand personal data protection by considering these dimensions: (1) Privacy and digital rights: Internet use by children leaves significant digital traces, making them vulnerable to data misuse. Data gathering and protection are governed by strict privacy laws like the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA). Companies must obtain parental consent before collecting children's data [1, 2]. Privacy issues and targeted advertising may arise from unregulated data tracking. Protecting digital rights prevents exploitation and encourages online ethics. Children's digital autonomy is safeguarded by privacy. Transparency makes the internet safer and more responsible for kids. (2) Identity theft and cybercrime prevention: Cybercriminals often target children's personal information. Hackers create fake accounts using stolen data that can go unnoticed for years. Secure data encryption and authentication reduce risks. Monitoring digital platforms helps detect and prevent unauthorized access. Cyber safety education helps kids become aware and secure online [3, 4]. Governments must tighten cybersecurity laws to protect children. Protecting children from identity theft safeguards their digital future. Keep yourself safe online: Online tracking and data collection manipulate and invade children's privacy. By showing individuals inappropriate content, algorithms can affect their internet experiences. Cyberbullying and exploitation thrive in unprotected internet contexts. Data protection limits hazardous interactions and prevents illegal access. The internet safety regulations protect children from digital harm and abuse. Parents must supervise their children's internet use to ensure their safety. Well-regulated digital spaces foster healthy online behavior in kids [5-7].

Legal frameworks provide ethical guidelines for collecting and using children's data. Companies must observe COPPA to avoid penalties for abuse. Security measures such as encryption and restricted access prevent data leaks. Educational institutions must have explicit data privacy rules to protect children. Parents and teachers should educate children on digital etiquette. Secure digital learning environments enhance trust in technology-based education. Student data and academic integrity are safeguarded by proper security measures. Growing parental control and awareness: Many parents are unaware of how their children's data is used online. Digital literacy lessons can assist parents in protecting their children's privacy. Parental control tools help limit children's internet usage. Internet safety is promoted by teaching children about potential risks.

Reasonable child data protection policies boost digital service trust. Transparent data practices reassure parents and educators about digital platforms. Businesses should prioritize privacy for ethical data collection. Governments must regulate businesses to protect children's data. More kid-friendly digital settings are coming. Trustworthy platforms improve kids' internet safety and experience. Data security helps kids and families trust digital services. In particular, the Vietnamese government's Draft Decree on addressing administrative violations in personal data privacy is crucial to improving the existing legislation's deterrent and efficacy. This proposal provides harsh penalties for failing to secure personal data, especially children's. Adding handling measures to the law will protect children's privacy and clarify digital firms' legal environment [8, 9].

Vietnam's regulations must be compared to developed countries like the U.S. with the Children's Online Privacy Protection Act (COPPA) and the EU with the General Data Protection Regulation (GDPR) to identify current limitations and propose solutions to improve children's privacy protection. This article reviews Vietnam's child personal data protection laws and adds international and Draft Decree observations and recommendations. The goal is to present a comprehensive perspective and recommend modifications to strengthen the legislative framework for children's personal data protection in the digital era. Based on the research, the study uses structural equation modeling (SEM) to quantify the effects of crucial elements on children's personal data protection. The paper presents a holistic framework for analyzing children's digital security vulnerabilities and policies by suggesting crucial policy recommendations incorporating legal, technological, and social factors.

2. Literature Review and Hypotheses Development

2.1. Children's Personal Data Protection (PD)

Child data protection is a set of legal, technical, and organizational procedures designed to protect the privacy and security of children's personal information in both digital and real-world settings. Children's personal data consists of directly identifiable information such as name, address, date of birth, and phone number, and indirectly recognizable data such as browsing history, geolocation, and online behavior [10, 11]. Child data protection is not only a technical issue; it is also a legal right, as emphasized in documents such as the United Nations Convention on the Rights of the Child (UNCRC), the EU's General Data Protection Regulation (GDPR), and the United States Children's Online Privacy Protection Act (COPPA). In Vietnam, child data protection is governed by the Vietnam [12] and the Vietnam [13], which provide criteria for collecting, processing, and storing children's data based on transparency, security, and parental/guardian consent [14]. Beyond the legislative framework, child data protection entails educating children, parents, and teachers about the dangers of sharing information online and adopting security technology to avoid data exploitation. The ultimate goal is to create a safe digital environment where children can access technology healthily while protecting their privacy rights.

2.2. Legal System (LS)

The legal system protects children's data privacy through laws, rules, and enforcement mechanisms. Global frameworks such as the UNCRC, GDPR, and COPPA set principles for children's online safety. In Vietnam, the Vietnam [12] and the Vietnam [13] govern data collection by requiring parental consent and secure storage [15, 16]. Legal provisions require transparency,

purpose limitation, and minimization to prevent improper data usage. Violations result in fines or legal action, and regulatory agencies enforce compliance. Technology companies must integrate child-friendly privacy controls, encryption, and restricted advertising to meet legal requirements. Beyond legislation, laws encourage education about digital risks, empowering children, parents, and educators [17, 18]. The legal system also fosters collaboration among governments, companies, and platforms to improve data security. Effective enforcement protects children's rights, resulting in a safer digital environment. Therefore, the authors proposed hypothesis H1 in Figure 1.

2.3. Coordination among Agencies (CA)

Effective coordination across authorities is critical for improving children's data protection, ensuring compliance, and tackling emerging threats in the digital realm. Collaboration among government agencies, regulatory authorities, law enforcement, educational institutions, and private entities enhances the enforcement of data privacy and child protection regulations [19, 20]. Regulatory institutions such as data protection authorities, cybersecurity units, and consumer protection bodies establish recommendations and enforce compliance with GDPR, COPPA, and Vietnam's [13]. Meanwhile, law enforcement agencies investigate violations, prosecute criminals, and combat cybercrime against children [21]. Educational institutions are essential in promoting digital literacy programs and informing children, parents, and educators about internet safety and appropriate data-sharing practices. Technology businesses and online platforms must adhere to privacy standards by establishing age-appropriate safeguards, parental controls, and secure data processing processes. Inter-agency coordination simplifies the international response to data privacy crimes [22]. Intelligence sharing, joint investigations, and alignment of laws prevent exploitation. Organizations can create a comprehensive child data protection framework that keeps children safe online by coordinating across sectors. Therefore, the authors proposed hypothesis H2 in Figure 1.

2.4. Awareness and Training (AT)

Teaching children, parents, educators, and organizations about digital privacy risks and obligations and awareness and training can improve kids' data security. Parental awareness programs teach parents to secure their children's data, identify online threats, manage privacy settings, and regulate internet use [23]. Digital literacy training in schools teaches pupils about cybersecurity, data protection, and safe online behavior. Mandatory training ensures enterprises and technology platforms comply with GDPR, COPPA, and Vietnam's Vietnam [13]. Child data handlers learn secure data collection, storage, and processing to reduce breaches and misuse [24, 25]. Law enforcement and government agencies use specialized training to enforce data protection laws and investigate cyber risks. Media and community seminars promote data safety [26]. By integrating awareness and training across sectors, societies can avoid data exploitation, boost compliance, and make children's digital lives safer. Therefore, the authors proposed hypothesis H3 in Figure 1.

2.5. Technology Development (TD)

In the digital age, technology expansion affects kids' data protection, providing benefits and concerns. Children's data is protected against unauthorized access via advanced encryption and cybersecurity. AI-powered content filtering removes harmful content, and parental control software allows parents to monitor and regulate their kids' online activities; rapid technical advancements are risky [27]. If unregulated, big data analytics, AI tracking, and targeted advertising increase the risk of data exploitation. Facial recognition and other biometrics present privacy and data usage concerns. GDPR, COPPA, and Vietnam's [13] require IT companies to comply [28, 29]. These regulations require age verification, transparency, and data minimization to avoid child data theft. Governments, IT companies, and educators must work together to maximize technology benefits [30]. Privacy-by-design, AI-driven threat detection, and cybersecurity can secure child data and make the internet safer. Therefore, the authors proposed hypothesis H4 in Figure 1.

2.6. Monitoring and Violation Handling (MV)

Enforcing child data protection laws and privacy guidelines requires effective monitoring and infringement redress. Governments, regulatory agencies, and technology companies must adopt effective supervision systems to detect, prevent, and respond to child data breaches [31]. Data protection authorities monitor compliance with GDPR, COPPA, and Vietnam's Personal Data Protection Decree. They audit, examine, and analyze risks within organizations to ensure child data security. Business data mistreatment is discouraged by harsh penalties and enforcement [32, 33]. Non-compliant firms must improve data protection due to fines, license revocations, and legal action. Public instances, such as computer corporations being fined millions for COPPA infractions, underscore the importance of vigorous enforcement. Legal measures and real-time monitoring tools, like AI-driven anomaly detection, help uncover breaches [34]. Platforms must also allow parents and children to report privacy issues easily. Continuous monitoring, strict enforcement, and public accountability improve child data protection frameworks, ensuring children's personal information is secured online. Therefore, the authors proposed hypothesis H5 in Figure 1.

Based on the abovementioned analysis, legal enforcement, technology, monitoring, awareness, and agency collaboration are all essential for protecting children's personal data. A solid legislative framework governs data collection, parental consent, and privacy protections. Agency coordination ensures efficient enforcement by bringing together government organizations, technology businesses, and law enforcement. This improves policy alignment and cross-border data protection initiatives. Raising awareness and training enables children, parents, and educators to spot internet hazards. To prevent data misuse, schools and organizations implement digital literacy programs and provide compliance training.

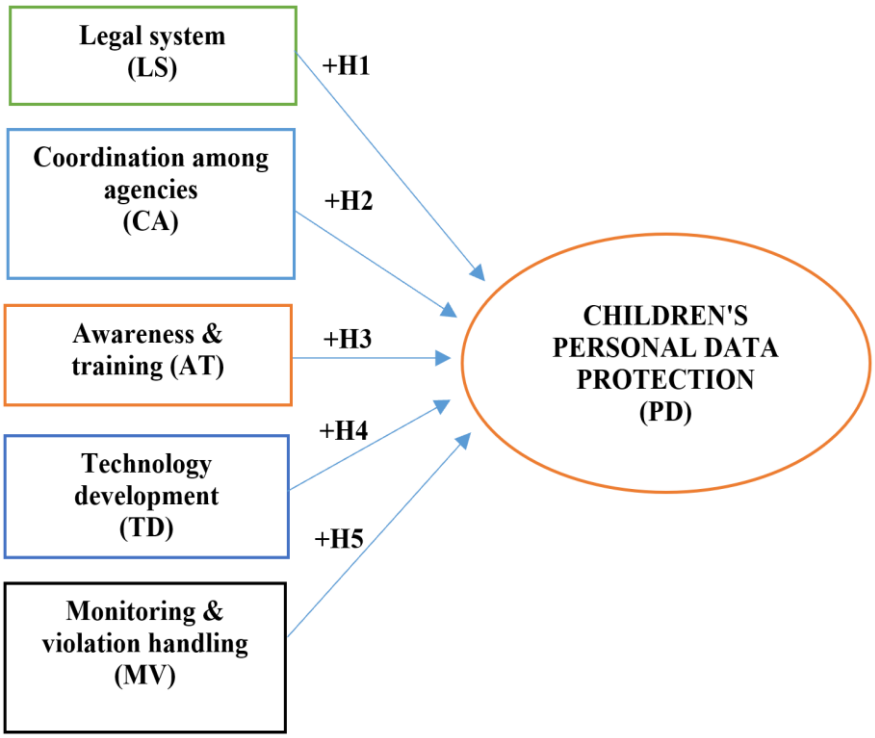

Figure 1.
A research model for critical factors influencing children's personal data protection in Vietnam.
Source: The authors proposed the model.

Figure 1 shows five key factors affecting children's personal data protection in Vietnam: legal system (LS), coordination among agencies (CA), awareness and training (AT), technology development (TD), and monitoring and violation handling (MV).

3. Research Methods

The authors created a process with these steps to conduct research, including step 1: Identify the research problem. Step 2: Build a theoretical framework and research overview. Step 3: Design the research method. Step 4: Build a survey questionnaire. Step 5: Validate and calibrate the research tools. Step 6: Collect data. Step 7: Process and analyze the data. Step 8: Present the research results. Step 9: Propose policy recommendations.

Step 1: Identify the research issue: With the rise of digitization, the study examines Vietnamese children's personal data protection. Cyberspace information insecurity threatens children, yet there is no legal or policy framework to protect them. Thus, this research evaluates existing rules, stakeholder knowledge, and modest personal data protection enforcement. The report also identifies policy loopholes and suggests enhancing minors' data protection. Study participants include parents, teachers, administrators, legal experts, and politicians. The report assesses the current situation in HCMC and provides practical solutions to improve children's personal data safety.

Step 2: The study's theoretical framework and literature review investigate Vietnamese and global legislation and policy frameworks for methodically and scientifically protecting children's personal data. The Cybersecurity Law, Decree on Personal Data Protection, and child rights rules will be assessed for efficacy and improvement. The study also compares these to GDPR (Europe) and COPPA (US) to learn from global experiences. Theories of data protection, privacy awareness, and policy enforcement will form the analytical foundation. Previous studies can reveal research gaps, enabling the creation of hypotheses and research topics relevant to Vietnam's current circumstances.

Step 3: Research methodology design: The study gathers data from many angles using qualitative and quantitative methods. The qualitative method involves in-depth interviews with ten child rights lawyers. These experts discuss legal challenges, policy enforcement, and reforms. Four hundred fifty people, two hundred parents, one hundred teachers, school administrators, fifty regulatory organization representatives, fifty parliamentarians, and fifty legal experts were polled for the quantitative method. Ho Chi Minh City will host the poll from October 2024 to January 2025. Surveys sent to target groups will collect data directly and indirectly.

Step 4: Create the survey questionnaire: The questionnaire uses a five-point Likert scale to assess factors linked to children's personal data protection (1 - Strongly Disagree, 5 - Strongly Agree). The content addresses significant issues such as parental and teacher understanding of data privacy, existing safeguards, the efficacy of the legislative framework, and coordination among regulatory bodies. Furthermore, the questionnaire includes open-ended questions to elicit qualitative comments from various respondent groups. Additionally, a distinct set of questions will be developed for in-depth interviews with legal experts, emphasizing policy loopholes and enforcement procedures. The questionnaire design process undergoes preliminary validation to guarantee clarity and ease of understanding for responders [35].

Step 5: Research instrument validation and refinement to guarantee clarity and relevance; a small group of 10-20 people will test the questionnaire before a large-scale survey. The pilot test identifies errors and ambiguities, allowing for quick changes. Scale internal consistency will be assessed using reliability tests like Cronbach's Alpha if needed. Qualitative interview questions will be evaluated to ensure expert opinions are collected appropriately. Before the formal survey, this technique optimizes research instruments to provide reliable data collection.

Step 6: In-depth expert interviews and a large-scale survey of 450 respondents will be used to collect data. The study team will interview ten legal experts personally or online using a script for the qualitative method. The quantitative technique will send respondents the survey questionnaire via paper mail. The research team will monitor progress, encourage respondents to complete the survey, and check responses during data collection. The qualitative study was tested with 10 legal management experts. After modifying the questionnaire, we performed large-scale polls in Ho Chi Minh City. The writers discussed 450 survey responses. Email and phone surveys were sent. The survey included 200 parents, 100 teachers and education managers, 50 management agency officials, 50 policymakers, and 50 legal experts. The total number of survey participants was 450, mostly from Ho Chi Minh City. Questionnaires are mailed to respondents from October 2024 to January 2025.

Step 7: Data processing and analysis: The authors used convenient and online sampling methods to conduct the quantitative study with 450 respondents based on the questionnaire, expecting a 96.67% response rate and 435 valid responses from 450 questionnaires distributed via email and direct methods. Data were processed using the questionnaire, cleaned, and loaded into the software. Descriptive statistical results combined qualitative and quantitative analysis to better understand children's personal data protection. The material is processed and analyzed following data gathering to obtain research conclusions. The qualitative data from in-depth interviews will be synthesized, classified into significant themes, and reinforced by expert quotes [35].

Step 8: Presenting research findings: Based on formal quantitative research, the authors used AMOS for SEM analysis and validation. The CFA confirmatory factor analysis study encompassed the entire scale. The authors used 435 valid samples from a quantitative survey of 450 respondents. Most management of the above companies were surveyed via email using random convenience sampling. The sample size was determined by the processing technique for Cronbach's Alpha greater than 0.7, as specified by EFA, SEM, etc., and measured model fit with GFI $\geq$ 0.900, TLI $\geq$ 0.900, CFI $\geq$ 0.900, and RMSEA $<$ 0.1.

Step 9: Policy recommendations: The authors provide specific recommendations to improve children's personal data protection based on the research findings. These recommendations may include enhancing the legislative framework, increasing public awareness, and investing in security technologies. The proposals will be created based on scientific data and their viability in Vietnam.

Table 1.
Testing of Cronbach's Alpha for factors affecting children's personal data protection.

Items	Min.	Max.	Cronbach's Alpha	Mean	Std. Deviation
Legal system (LS)			0.926	3.083	0.956
LS1	1	5	0.898	3.069	0.958
LS2	1	5	0.911	3.078	0.981
LS3	1	5	0.886	3.131	0.928
LS4	1	5	0.920	3.053	0.957
Coordination among agencies (CA)			0.834	3.521	0.872
CA1	1	5	0.781	3.552	0.831
CA2	1	5	0.773	3.605	0.875
CA3	1	5	0.827	3.425	0.921
CA4	1	5	0.780	3.503	0.860
Awareness & training (AT)			0.927	3.103	0.980
AT1	1	5	0.898	3.101	0.997
AT2	1	5	0.904	3.115	0.979
AT3	1	5	0.898	3.152	0.936
AT4	1	5	0.920	3.044	1.007
Technology development (TD)			0.799	2.401	0.685
TD1	1	5	0.777	2.336	0.723
TD2	1	5	0.711	2.412	0.628
TD3	1	5	0.787	2.402	0.687
TD4	1	5	0.719	2.455	0.702
Monitoring & violation handling (MV)			0.943	3.039	0.969
MV1	1	5	0.918	3.030	0.956
MV2	1	5	0.928	3.005	0.986
MV3	1	5	0.934	3.094	0.925
MV4	1	5	0.920	3.028	1.011
Personal data protection (PD)			0.690	3.309	0.995
PD1	1	5	0.572	3.556	0.900

PD2	1	5	0.556	3.264	1.008
PD3	1	5	0.667	3.106	1.077

4. Research Results and Discussions

4.1. Testing Critical Factors Affecting Children's Personal Data Protection in Vietnam

Table 1 shows the findings of Cronbach's Alpha reliability testing for numerous elements that influence children's personal data protection. The analysis includes each construct's internal consistency and descriptive statistics, such as the mean and standard deviation.

The legal system (LS): The legal system plays an essential role in safeguarding children's personal information by setting legislation and enforcement measures. A high Cronbach's alpha (0.926) indicates excellent internal consistency in responses. With a mean score of 3.083, the legal framework is rated as moderately effective. However, responses (standard deviation ~0.95) show varying perspectives on enforcement. Strengthening legal compliance and addressing loopholes could improve data security.

Coordination among agencies (CA): Effective agency coordination increases data protection efforts through collaboration and policy alignment. Cronbach's Alpha of 0.834 suggests high internal consistency. The mean score of 3.521 indicates that interagency cooperation is relatively strong. However, the variability in replies (std. deviation ~0.86) indicates areas for improvement. Improving communication and establishing defined responsibilities can boost effectiveness. A centralized regulatory authority may facilitate cooperation.

Awareness and training (AT): initiatives educate stakeholders on data protection threats and effective practices. Cronbach's Alpha (0.927) indicates outstanding reliability, demonstrating the strong consistency of responses. Awareness efforts are rated moderately effective, with a mean score of 3.103. The high standard deviation (~1.00) indicates diverse knowledge levels among respondents. Expanding outreach efforts could help raise public awareness. Integrating digital literacy into education may help young people understand data privacy.

Technological development (TD): Technology is essential in protecting children's personal information, yet current improvements are insufficient. Cronbach's Alpha (0.799) indicates acceptable dependability but is lower than other criteria. A mean of 2.401 suggests that respondents regard technological interventions as ineffective. The low standard deviation (~0.7) indicates ongoing concerns about inadequate cybersecurity. Improving encryption and authentication tools can reduce hazards. Investment in data security innovations is required for improvement.

Monitoring and violation handling (MV): Effective monitoring and enforcement measures ensure compliance with data protection standards. A high Cronbach's Alpha (0.943) indicates excellent internal consistency in responses. The mean score of 3.039 indicates modest trust in the existing monitoring efforts. However, substantial standard deviations (~1.0) show differences in views of enforcement efficacy. Strengthening oversight systems can improve accountability. The prompt and honest resolution of infractions reinforces trust. Implementing more significant penalties for noncompliance may act as a deterrent.

Children's personal data protection (PD): The ultimate purpose of these procedures is to secure personal data while ensuring children's privacy and security. Cronbach's alpha of 0.690 indicates moderate reliability, with room for improvement. The average score of 3.309 indicates a fair impression of current protective measures. High standard deviations (~1.0) suggest inconsistent experiences among respondents. Strengthening privacy legislation and ensuring efficient implementation are required.

Moreover, structural equation modeling (SEM) results examine the impact of five key factors on children's personal data protection (PD). The model evaluates standardized estimates, critical ratios (C.R.), significance levels (P-values), and hypothesis acceptance. All five hypotheses (H1-H5) are accepted, indicating that each factor significantly impacts personal data protection Table 2.

Table 2.
Testing SEM model for factors affecting children's personal data protection in Vietnam.

Relationships			Standardized Estimate	Estimate	S.E	C.R	P	Hypothesis	Result
LS	→	PD	0.478	0.334	0.047	7.143	***	H1	Accepted
CA	→	PD	0.186	0.148	0.046	3.218	0.001	H2	Accepted
AT	→	PD	0.128	0.068	0.023	2.894	0.004	H3	Accepted
TD	→	PD	0.124	0.223	0.074	3.037	0.002	H4	Accepted
MV	→	PD	0.129	0.112	0.041	2.741	0.006	H5	Accepted

Note: *** significance at 0.01.

Table 2 shows the testing SEM model for factors influencing children's personal data protection in Vietnam.

Legal system (LS) → Personal data protection (PD): The legal system is the most critical factor in protecting children's data. With a normalized estimate of 0.478, it has the most significant influence of all components. Strict laws, transparent policies, and efficient enforcement are critical to guaranteeing compliance. A high critical ratio (C.R. = 7.143, $P < 0.001$) indicates a significant influence. Weak enforcement may result in data vulnerabilities. Strengthening legal structures can improve protection. Regular policy revisions are required to respond to emerging cyber dangers.

Coordination among agencies (CA) → Personal data protection (PD): Inter-agency collaboration is required for a comprehensive data protection strategy. A moderate standardized estimate (0.186, C.R. = 3.218, P = 0.001) demonstrates its

relevance. Better coordination among government entities, corporate organizations, and non-governmental organizations (NGOs) can help to close regulatory gaps. Inconsistent policies may undermine enforcement attempts. Improving communication channels can facilitate information sharing. A centralized monitoring body can ensure more efficient enforcement. Precise accountability mechanisms will result in improved execution.

Awareness & training (AT) → Personal data protection (PD): Public awareness and training programs shape responsible data management behaviors. With a standardized estimate of 0.128 (C.R. = 2.894, P = 0.004), its effect is statistically significant but relatively small. Educational initiatives, conferences, and school curricula can help raise awareness. Lack of information exposes children and parents to cyber hazards. More funding for digital literacy programs is required. Training service providers can help strengthen data security procedures. A proactive approach can improve long-term protection.

Technology development (TD) → Personal data protection (PD): Technology can help protect children's personal data. A standardized estimate of 0.124 (C.R. = 3.037, P = 0.002) supports its importance. Advancements in encryption, authentication, and data security can help to mitigate risks. Children who are slow to learn new technologies may be vulnerable to cyber dangers. More investment in privacy-enhancing technologies (PETs) is required. Regular security infrastructure changes are critical for responding to developing threats. To provide better protection, technological solutions must be aligned with legislative frameworks.

Monitoring and violation handling (MV) → Personal data protection (PD): A robust monitoring mechanism assures compliance with data protection rules. With a standardized estimate of 0.129 (C.R. = 2.741, P = 0.006), it is critical. Data breaches can be detected and responded to promptly to prevent future misuse. Weak enforcement may foster noncompliance among organizations. More substantial fines and oversight systems are required for deterrence. Transparency in violation handling increases public trust. Continuous evaluation of policies can enhance long-term efficacy.

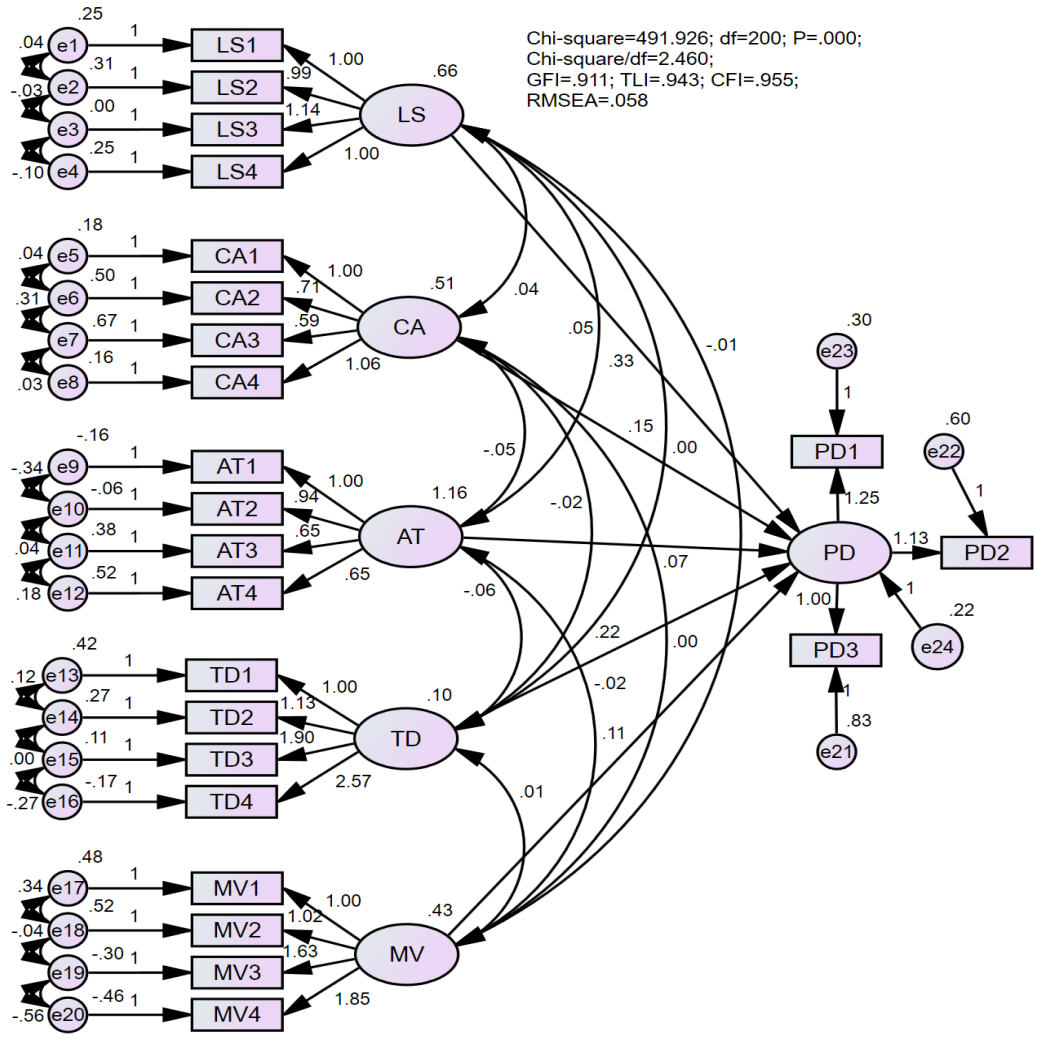

Figure 2.
Testing SEM for factors influencing children's personal data protection in Vietnam.

Figure 2 depicts the significance threshold of 0.05 for assessing five essential components of children's personal data protection in Vietnam. The following statistical metrics measured the model's fit: GFI = 0.911 (>0.850), TLI = 0.943 (>0.900), CFI = 0.955 (> 0.900), and RMSEA = 0.058 (< 0.1). To understand the interrelationships of the most important variables impacting the children's personal data protection in Vietnam, the researchers used structural equation modeling (SEM) with SPSS 20.0 and Amos, as shown in the image.

Table 3.
Testing average variance extracted for factors influencing children's personal data protection.

Code	CR	AVE	MSV	Results
TD	0.807	0.517	0.069	Good
MV	0.944	0.807	0.019	Good
LS	0.927	0.761	0.261	Good
AT	0.928	0.763	0.069	Good
CA	0.831	0.559	0.030	Good
PD	0.757	0.518	0.261	Good

With CR = 0.807 and AVE = 0.517, technology development (TD) scarcely affects child data protection (Table 3). A low MSV (0.069) indicates low component overlap. Investment in cybersecurity and encryption improves security. Privacy-enhancing technologies (PETs) need constant updates. Monitoring and Violation Handling (MV) is strongest (CR = 0.944, AVE = 0.807). Few things affect 0.019 MSV. Strict enforcement and quick response boost compliance. More severe data breach fines may deter. The legal system (LS) impacts data protection the most (CR = 0.927, AVE = 0.761, MSV = 0.261). High MSV significantly suggests PD. A strong legal system ensures accountability and enforcement. Data protection for minors can be improved by policy implementation. Awareness and training (AT): AT produces low MSV (0.069) but substantial dependability (CR = 0.928, AVE = 0.763). Data privacy threats require public education. Digital literacy lowers risks. Help stakeholders use data protection processes consistently. Coordination between agencies: PD's substantial dependability (CR = 0.831, AVE = 0.559) and low MSV (0.030) limit its link to coordination. Policy gaps can be filled via partnerships. Task streamlining boosts enforcement. Centralized regulation may improve coordination. Legal enforcement makes personal data protection moderately dependable (CR = 0.757, AVE = 0.518, MSV = 0.261). Data privacy laws must be strengthened. Security audits highlight flaws. Proper digital actions boost security. Table 3 illustrates each component's composite reliability (CR), average variance extracted (AVE), and maximum shared variance (MSV) for children's PD. All constructions have CRs over 0.7 and AVEs over 0.5, indicating good internal consistency and convergence.

Table 4.
Testing Bootstrap 50.000 samples for factors influencing children's personal data protection.

Parameter			SE	SE-SE	Mean	Bias	SE-Bias	C.R	Results
LS	→	PD	0.064	0.001	0.325	0.004	0.003	1.33	Accepted H1
CA	→	PD	0.063	0.001	0.137	0.001	0.002	0.50	Accepted H2
AT	→	PD	0.028	0.001	0.062	0.006	0.005	1.20	Accepted H3
TD	→	PD	0.093	0.002	0.196	0.007	0.004	1.75	Accepted H4
MV	→	PD	0.051	0.001	0.118	0.007	0.005	1.40	Accepted H5

Table 4 shows the results of Bootstrap testing on 50,000 samples to validate the links between five critical parameters and personal data protection (PD). The model evaluates standard error (SE), bias, and critical ratio (CR) to ensure the robustness of the findings. All hypotheses (H1–H5) are accepted, confirming that each factor strongly affects PD.

4.2. Discussion of Findings

Based on reliability, validity, and structural equation modeling (SEM), this study identifies key determinants impacting children's personal data protection in Vietnam. Policymakers and managers can benefit from the findings, which show strong connections between LS, CA, AT, TD, and MV and highlight that legal enforcement and inter-agency coordination play the most crucial roles in children's data protection. While awareness, technology, and monitoring efforts are essential, they require further strengthening to maximize effectiveness. Future efforts should focus on integrating legal, technical, and educational measures to establish a comprehensive data protection framework.

(1) Legal system (LS) → Personal data protection (PD): The legal system (LS) has the most significant impact on children's data protection (Standardized estimate = 0.478, P < 0.001, in Table 2). A high Cronbach's Alpha (0.926) indicates excellent internal consistency and reliable replies [3, 8, 15, 33]. Clear legislation and rigorous enforcement procedures are critical for protecting personal information. The strong link with PD indicates that comprehensive rules considerably improve data security. Weak enforcement might create legal loopholes, exposing minors to cyber risks.

(2) Coordination among agencies (CA) → Personal data protection (PD): Inter-agency coordination (CA) had a moderate impact on protecting children's data (standardized estimate = 0.186, P = 0.001, in Table 2). Cronbach's Alpha (0.834) implies high dependability, confirming consistent results. Effective communication and collaboration among regulatory organizations ensure that policies are consistently applied [4, 7, 18, 21]. Weak interagency coordination can result in fragmented enforcement, decreasing the effectiveness of legal systems. The alignment of government institutions, corporate organizations, and non-governmental organizations (NGOs) is critical for addressing regulatory gaps. A centralized monitoring body can increase coordination by defining explicit rules. Cross-sector collaboration can improve data security by combining technological, legal, and awareness activities.

(3) Awareness & training (AT) → Personal data protection (PD): Awareness and training (AT) has a considerable impact on children's data protection, but not as much as the legal system (Standardized Estimate = 0.128, P = 0.004, in Table 2).

High dependability (Cronbach's Alpha = 0.927) implies that respondents regularly view awareness initiatives as critical [6, 14, 23, 26]. Educating children, parents, and educators about data privacy risks is crucial to preventing data exploitation. A lack of understanding exposes children to potential cyber risks. Digital literacy initiatives must be included in school curricula to teach ethical online activity. Training sessions for firms that handle children's data help improve compliance. Service providers should be compelled to comply with strict privacy training rules.

(4) Technology development (TD) → Personal data protection (PD): Technology development has a positive but more negligible impact on children's data protection (Standardized Estimate = 0.124, P = 0.002, in Table 2). Moderate reliability (Cronbach's Alpha = 0.799) indicates that, while technology plays an important role, it is not entirely optimized. Advancements in cybersecurity, such as encryption and AI-based threat detection, have the potential to significantly improve data security [11, 20, 27, 30]. Low adoption of privacy-enhancing technologies (PETs) reduces protection and increases danger. Increased investment in cybersecurity infrastructure is essential to improve internet safety, and governments should ensure safe data storage and transmission procedures. To protect personal information, technology companies should prioritize child-friendly privacy settings. Regular software updates and vulnerability checks can help avoid cyberattacks.

(5) Monitoring & violation handling (MV) → Personal data protection (PD): Monitoring and violation handling (MV) are crucial for complying with data protection rules (standardized estimate = 0.129, P = 0.006, in Table 2). A high Cronbach's Alpha (0.943) indicates that respondents believe monitoring is very effective in data protection. Regular audits and compliance inspections can discourage firms from breaking privacy laws [15, 18, 28, 33, 34]. Companies can exploit children's data without fear of repercussions due to weak enforcement. To increase accountability, strict sanctions for noncompliance must be implemented. Creating real-time monitoring systems can assist in detecting and responding to data breaches quickly. Public reporting systems should be developed to encourage transparency in managing infractions.

5. Conclusions and Policy Recommendations

5.1. Conclusions

The paper stresses the importance of strong legal frameworks, interagency coordination, and technical advances to secure Vietnamese children's personal data. Legislators, educators, and digital service providers must secure data when kids use the internet. The structural equation modeling (SEM) research shows that the legal system, agency collaboration, awareness and training, technology development, monitoring, and violation management improve children's data protection. Legal systems have the most significant impact, highlighting the necessity for clear policies and strict enforcement. Existing laws establish data security, but execution gaps, fragmented norms, and insufficient awareness prevent effective protection. Better inter-agency collaboration is needed to execute policies faster and comply with regulations. Public awareness campaigns should also educate children, parents, and service providers about data privacy. Technology improves security, yet privacy-enhancing solutions are delayed. Investment in modern cybersecurity infrastructure, AI-driven threat detection, and encryption solutions improves digital security. Enhance monitoring and violation resolution, including harsher compliance inspections and higher data breach fines. The paper offers several critical policy proposals to address these issues: (1) Establishing a personal data protection commission to oversee data security. (2) Unifying data protection laws into a single personal data protection act for regulatory consistency. (3) Raising penalties for noncompliance to match international data protection standards. (4) Expanding digital literacy programs to educate stakeholders about data protection. (5) Promoting cybersecurity to reduce digital risks. These strategic ideas may help Vietnam establish a long-term, effective data protection system for children's personal data in the digital age. Policymakers, regulators, and digital service providers must work together to secure the Internet for future generations' privacy and digital rights.

5.2. Policy Recommendations

The results of the structural equation modeling (SEM) show that five essential elements influence children's personal data protection (PD) in Vietnam. The standardized estimates in Table 2 show each factor's influence strength. Based on these findings, the following policy proposals are recommended to improve the data protection for children:

(1) Strengthening legal system (LS → PD: 0.478): The legal system has the most significant impact (0.478, P < 0.001, in Table 2) on children's data protection. A uniform Personal Data Protection Act should be implemented to replace the current patchwork of legislation. Stricter enforcement and heavier sanctions are required to dissuade infractions. Independent regulatory organizations should monitor compliance and resolve enforcement loopholes. To safeguard data security, online platforms must adopt child-specific privacy measures. To keep up with increasing cyber threats, policies must be updated frequently. Cross-sector collaboration can increase the effectiveness of legal enforcement. Increasing legal understanding among digital service providers will improve compliance. International data protection standards should be implemented to strengthen Vietnam's regulatory framework. A robust legal framework ensures accountability, uniformity, and trust in digital safety. This means that parents will have full decision-making authority for all matters relating to the processing of personal data of children from 0 to under 13 years of age. Upon reaching age 13 or older, children will be entitled to make their own decisions regarding the consent of their personal data. This approach ensures the necessary protection for children in a complex digital environment while fostering a sense of responsibility in children for the safety of their own personal data. Drawing on the experience of COPPA, which requires parental consent for children under 13, and GDPR, which requires parental consent for children under 16 (with some member states allowing adjustments down to 13), Vietnam should consider adjusting the age of consent accordingly.

(2) Enhancing coordination among agencies (CA → PD: 0.186): Inter-agency collaboration has a moderate influence (0.186, P = 0.001, in Table 2) but is still an essential aspect of good data protection. A single Personal Data Protection Commission should be established to oversee enforcement and streamline legislation. A national data-sharing network can

help increase communication among government departments, corporations, and non-governmental organizations (NGOs). To achieve a cohesive strategy, regulatory overlap and inconsistencies must be addressed. Joint training programs can help authorities coordinate their enforcement activities. Cross-border coordination is critical for protecting children's data from foreign cyberattacks. Creating a uniform reporting system will improve response times to data breaches. Public-private collaborations should be strengthened to encourage shared accountability. Clarifying legal obligations among agencies ensures that enforcement is effective. An integrated strategy will increase regulatory efficiency and policy consistency. Vietnam should consider establishing an independent Personal Data Protection Commission specifically responsible for personal data protection, similar to the EU or US models. This Personal Data Protection Commission would be responsible for supervising, guiding, and enforcing regulations related to personal data protection while also providing support to individuals and organizations in complying with the law through the establishment of an independent Personal Data Protection Commission that strengthens the monitoring mechanism to ensure the enforcement of laws on children's personal data protection, including through random inspections and investigations of potential violations. This Commission will be the enforcement and administrative sanctioning competent authority for personal data protection issues and children's personal data protection. This avoids overlap and complexity in sanctioning violations in this field due to complete expertise in detecting, evaluating, and handling violations.

(3) Strengthening monitoring & violation handling (MV → PD: 0.129): Monitoring measures have a significant impact (0.129, P = 0.006, in Table 2) on compliance and responsibility. To dissuade careless behavior, strict fines for data breaches should be applied. Regular compliance assessments of digital platforms will increase conformity to privacy rules. An impartial data protection oversight council should be formed to oversee enforcement. A real-time violation detection system can track and address breaches as soon as they occur. Public reporting systems should be made available to promote openness and accountability. Technology businesses must be obliged to provide annual privacy compliance reports. Whistleblower protection legislation should be enacted to help employees who disclose wrongdoing. A transparent appeals process should be established to handle data-related issues. Strict monitoring and vigorous enforcement foster a trustworthy digital environment. The public disclosure of violations involving children's personal data will enhance transparency and establish important legal precedents for future cases. This approach also helps the community better understand the importance of personal data protection. Finally, Vietnam should strengthen international cooperation in protecting children's personal data by learning from countries with advanced legal systems and participating in international conventions related to privacy and personal data protection.

(4) Expanding awareness & training (AT → PD: 0.128): Despite having a reduced impact (0.128, P = 0.004, in Table 2), awareness and training remain critical for preventing data breaches. Digital literacy initiatives should be increased to educate children, parents, and educators on internet privacy threats. Data protection awareness must be integrated into school curricula to establish safe online practices for children. Businesses and service providers can benefit from training seminars to ensure compliance with privacy legislation. Public communication campaigns should be conducted to educate users on their data rights. Parents must have tools to monitor and protect their children's online activity. Partnerships with media and technology businesses can help to raise privacy awareness more effectively. Service providers should be required to post transparent privacy policies for customers. Mandatory data protection certification programs can help raise industry standards. Well-informed individuals are better suited to protect their personal information. Vietnam should consider promulgating a specific law on personal data protection, with clear and detailed provisions on children's rights, the responsibilities of organizations and individuals, and specific protection measures in the digital environment. When Vietnam promulgates a particular law, it will ensure comprehensive and specific protection. The law should include provisions on collecting, processing, storing, and protecting children's personal data, require parental consent, and clearly outline the responsibilities of organizations and individuals in children's personal data protection. Furthermore, a specific law on personal data processing will help synchronize the regulations on the issue of personal data protection that are currently scattered and overlapping in Vietnam.

(5) Advancing technology development (TD → PD: 0.124): With a moderate influence (0.124, P = 0.002, in Table 2), Technology is critical in protecting children's personal information. Enforcing encryption and secure authentication techniques will improve data security. Companies must use privacy-enhancing technologies (PETs) to prevent illegal data access. AI-powered cybersecurity technologies can detect and prevent possible threats in real-time. Strict controls should be imposed on technology corporations to ensure ethical data acquisition. Parental control tools should be improved to effectively monitor children's online behavior. Encouraging investment in cybersecurity research will assist in building more effective data protection mechanisms. Secure cloud storage solutions should be promoted to reduce data leaks. Standardized security protocols for digital platforms will lead to a safer online world. Technology-driven solutions must align with legal laws to be effective. The Government of Vietnam should implement policies that encourage, incentivize, and support organizations and businesses in adopting advanced security technologies for collecting, storing, and processing children's personal data. This includes data encryption, access management, and security system monitoring. Besides, Vietnam should develop specialized technical solutions to protect children online, such as privacy control tools, warning applications, and educational programs about the risks of information insecurity.

6. Limitations and Future Research

6.1. Limitations

Despite its importance, this study has several drawbacks. First, the sample is limited to Ho Chi Minh City, which may not adequately represent viewpoints from other parts of Vietnam, particularly rural areas with different internet availability and regulatory enforcement. A broader national sample would yield a more complete analysis. Second, the qualitative data is based on interviews with only ten legal professionals, which, while fascinating, do not reflect a diverse range of

perspectives, such as lawmakers, cybersecurity experts, and technology sector leaders. A broader expert panel could confirm the findings. Third, the paper examines Vietnam's regulatory system without comparing it to global data protection standards like GDPR or COPPA. Comparative legal studies may reveal best practices and regulatory gaps. Fourth, the report acknowledges the relevance of technology in data protection but does not examine progressive cybersecurity solutions like AI-driven security, privacy-enhancing technologies, or blockchain. Evaluating these technologies' acceptance and efficacy may improve results.

6.2. Future Research

Under these limits, future research should expand the scope and depth of the analysis to make more robust policy suggestions. First, expanding the sample outside Ho Chi Minh City to include rural and urban residents will improve generalizability. A broader, more diverse dataset may show regional digital literacy, internet availability, and data protection enforcement disparities. Second, comparing Vietnam's data protection laws to GDPR, COPPA, and ASEAN norms would identify strengths and weaknesses. This would allow policymakers to apply international best practices. Third, researchers should investigate how AI, blockchain, and PETs can secure children's data. Policymakers and technology providers can learn from the implementation, adoption, and data protection effectiveness of these solutions. Fourth, longitudinal research should examine how changes in legislation and enforcement affect children's data protection. Such investigations can evaluate whether new data privacy laws reduce threats or if more revisions are needed. Fifth, studies should examine how social media and internet companies manage children's data. Their compliance with data protection laws and privacy policies can help determine if stricter measures are needed to hold businesses accountable.

References

[1] I. Milkaite and E. Lievens, "Children's rights to privacy and data protection around the world: Challenges in the digital realm," *European Journal of Law and Technology*, vol. 10, no. 1, pp. 1–24, 2019.

[2] Vietnam, *Law on handling administrative Violations, No. 15/2012/QH13, enacted April 20, 2012, amended by Law No. 67/2020/QH14, November 13, 2020*. Hanoi, Vietnam: National Assembly of the Socialist Republic of Vietnam, 2012.

[3] D. Smyr and E. Ulianova, "Legal issues of children's personal data protection," *Open Journal of Legal Studies*, vol. 5, no. 1, pp. 1–10, 2022. https://doi.org/10.32591/coas.ojls.0501.01001s

[4] A. Sofian, B. Pratama, and Besar, "Children's privacy and data protection in judicial decisions in Indonesia," *US-China Law Review*, vol. 18, no. 4, pp. 153–161, 2021. https://doi.org/10.17265/1548-6605/2021.04.001

[5] H. Pearce and C. Buck, "Balancing the autonomy and protection of children: Competency challenges in data protection law," *Information & Communications Technology Law*, vol. 33, no. 2, pp. 177-197, 2024. https://doi.org/10.1080/13600834.2024.2320978

[6] S. Livingstone and K. R. Sylwander, "There is no right age! The search for age-appropriate ways to support children's digital lives and rights," *Journal of Children and Media*, vol. 19, no. 1, pp. 6-12, 2025. https://doi.org/10.1080/17482798.2024.2435015

[7] M. Stoilova, R. Nandagiri, and S. Livingstone, "Children's understanding of personal data and privacy online–a systematic evidence mapping," *Information, Communication & Society*, vol. 24, no. 4, pp. 557-575, 2021. https://doi.org/10.1080/1369118X.2019.1657164

[8] S. Varadan, "The principle of evolving capacities under the UN convention on the rights of the child," *The International Journal of Children's Rights*, vol. 27, no. 2, pp. 306-338, 2019. https://doi.org/10.1163/15718182-02702006

[9] E. Stoycheff and J. Stoycheff, "The custodians of childrens' online privacy: Extending the APCO framework to parental social media sharing," *Communication Research and Practice*, vol. 10, no. 1, pp. 76-91, 2024. https://doi.org/10.1080/22041451.2024.2322815

[10] R. Barnes and A. Potter, "Sharenting and parents' digital literacy: An agenda for future research," *Communication Research and Practice*, vol. 7, no. 1, pp. 6-20, 2021. https://doi.org/10.1080/22041451.2020.1847819

[11] R. Das, "Parents' understandings of social media algorithms in children's lives in England: Misunderstandings, parked understandings, transactional understandings and proactive understandings amidst datafication," *Journal of Children and Media*, vol. 17, no. 4, pp. 506-522, 2023. https://doi.org/10.1080/17482798.2023.2240899

[12] Vietnam, *Law on cybersecurity (Law No. 24/2018/QH14)*. Hanoi: National Assembly of the Socialist Republic of Vietnam, 2015.

[13] Vietnam, *Decree on personal data protection (Decree No. 13/2023/ND-CP)*. Hanoi: Government of the Socialist Republic of Vietnam, 2023.

[14] A. K. Fox and M. G. Hoy, "Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers," *Journal of Public Policy & Marketing*, vol. 38, no. 4, pp. 414-432, 2019. https://doi.org/10.1177/0743915619858290

[15] I. N. Rezende, "The proposed Regulation to fight online child sexual abuse: an appraisal of privacy, data protection and criminal justice issues," *International Review of Law, Computers & Technology*, vol. 38, no. 3, pp. 369-390, 2024. https://doi.org/10.1080/13600869.2024.2324548

[16] I. Milkaite and E. Lievens, "Child-friendly transparency of data processing in the EU: from legal requirements to platform policies," *Journal of Children and Media*, vol. 14, no. 1, pp. 5-21, 2020. https://doi.org/10.1080/17482798.2019.1701055

[17] M. Oswald, H. James, and E. Nottingham, "The not-so-secret life of five-year-olds: Legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media," *Journal of Media Law*, vol. 8, no. 2, pp. 198-228, 2016. https://doi.org/10.1080/17577632.2016.1239942

[18] S. Holiday, M. S. Norman, and R. L. Densley, "Sharenting and the extended self: Self-representation in parents' Instagram presentations of their children," *Popular Communication*, vol. 20, no. 1, pp. 1-15, 2022. https://doi.org/10.1080/15405702.2020.1744610

[19] L. Belli and N. Zingales, "Cooperation and innovation to build meaningful data protection in Latin America," *International Review of Law, Computers & Technology*, vol. 39, no. 1, pp. 1-5, 2025. https://doi.org/10.1080/13600869.2024.2351670

[20] N. Isokuortti, "Organizational and systems factors impacting the adaptation of a child welfare practice model from the UK to Finland," *Human Service Organizations: Management, Leadership & Governance*, vol. 48, no. 4, pp. 474-495, 2024. https://doi.org/10.1080/23303131.2024.2304897

[21] E. Aaltio and N. Isokuortti, "Developing a programme theory for the systemic practice model in children's social care: Key informants' perspectives," *Child & Family Social Work*, vol. 27, no. 3, pp. 444-453, 2022. https://doi.org/10.1111/cfs.12896

[22] P. Gillingham, "Evaluation of practice frameworks for social work with children and families: Exploring the challenges," *Journal of Public Child Welfare*, vol. 12, no. 2, pp. 190-203, 2018. https://doi.org/10.1080/15548732.2017.1392391

[23] J. C. Andrews, K. L. Walker, and J. Kees, "Children and online privacy protection: Empowerment from cognitive defense strategies," *Journal of Public Policy & Marketing*, vol. 39, no. 2, pp. 205-219, 2020. https://doi.org/10.1177/0743915619883638

[24] J. Henriksen-Bulmer, E. Rosenorn-Lanng, S. Corbin-Clarke, S. Ware, D. Melacca, and L.-A. Fenge, "Using game-based learning to teach young people about privacy and online safety," *Interactive Learning Environments*, vol. 32, no. 10, pp. 6430-6450, 2024. https://doi.org/10.1080/10494820.2023.2265424

[25] P. Cardoso, D. V. Hawk, and D. Cross, "What young people need to make better-informed decisions when communicating with digital images: Implications for mental health and well-being," *Health Education & Behavior*, vol. 47, no. 1, pp. 29-36, 2020. https://doi.org/10.1177/1090198119885433

[26] G. He, "Distributed intelligent model for privacy and secrecy in preschool education," *Applied Artificial Intelligence*, vol. 37, no. 1, p. 2222494, 2023. https://doi.org/10.1080/08839514.2023.2222494

[27] S. J. Ball and E. Grimaldi, "Neoliberal education and the neoliberal digital classroom," *Learning, Media and Technology*, vol. 47, no. 2, pp. 288-302, 2022. https://doi.org/10.1080/17439884.2021.1963980

[28] R. Ribak, "Teens'"right to be let alone": Privacy under datafication," *Journal of Children and Media*, vol. 19, no. 1, pp. 53-57, 2025. https://doi.org/10.1080/17482798.2024.2438678

[29] D. Lupton and B. Williamson, "The datafied child: The dataveillance of children and implications for their rights," *New Media & Society*, vol. 19, no. 5, pp. 780-794, 2017. https://doi.org/10.1177/1461444816686328

[30] J. Savirimuthu, "Datafication as parenthesis: Reconceptualising the best interests of the child principle in data protection law," *International Review of Law, Computers & Technology*, vol. 34, no. 3, pp. 310-341, 2020. https://doi.org/10.1080/13600869.2019.1590926

[31] V. Chang, L. Golightly, Q. A. Xu, T. Boonmee, and B. S. Liu, "Cybersecurity for children: An investigation into the application of social media," *Enterprise Information Systems*, vol. 17, no. 11, p. 2188122, 2023. https://doi.org/10.1080/17517575.2023.2188122

[32] D. J. Power, C. Heavin, and Y. O'Connor, "Balancing privacy rights and surveillance analytics: A decision process guide," *Journal of Business Analytics*, vol. 4, no. 2, pp. 155-170, 2021. https://doi.org/10.1080/2573234X.2021.1920856

[33] G. Mascheroni, "Datafied childhoods: Contextualising datafication in everyday life," *Current Sociology*, vol. 68, no. 6, pp. 798-813, 2020. https://doi.org/10.1177/0011392118807534

[34] M. Padden and A. Öjehag-Pettersson, "Protected how? Problem representations of risk in the general data protection regulation (GDPR)," *Critical Policy Studies*, vol. 15, no. 4, pp. 486-503, 2021. https://doi.org/10.1080/19460171.2021.1927776

[35] J. Hair, R. Anderson, R. Tatham, and W. Black, *Multivariate data analysis*. Upper Saddle River, NJ, USA: Prentice-Hall, 2018.