Huynh Thi Truc, Giang
PhD, Deputy Head of the Department of Judicial Law
Can Tho University, Vietnam*

Nguyen Thi My, Linh
PhD, Director of the Center for Comparative Law
Can Tho University, Vietnam**

Doi: 10.15170/Dike.2026.10.01.02

From Traditional Ethics and Family Values to Postmodern Phenomena: The Evolution of Legislative Thinking on Children's Privacy in the Context of Digital Transformation in Vietnam

This article explores the evolution of Vietnamese legislative thinking on children's privacy rights, tracing a shift from a traditional framework rooted in family ethics and social norms towards legal responses to postmodern dynamics in the digital environment. In contemporary digital contexts, children are increasingly datafied, governed by algorithmic systems, and influenced by artificial intelligence. The article develops a historical analytical framework by examining the emergence of children's rights protection in international human rights instruments and analysing the processes through which these standards have been internalised in Vietnamese law. From a legal-historical perspective, it identifies three stages in the development of legislative thinking on children's privacy rights and exposes persistent limitations, notably the predominance of ex post regulatory responses and the absence of effective technological risk-management mechanisms. On this basis, the article proposes directions for legislative reform aimed at strengthening a child-centred approach that is responsive to the structural challenges of the digital environment.

Keywords: *children's privacy rights, legislative thinking, personal data protection*

1. Protecting children's rights in Vietnam: from historical foundations to digital-era challenges

The protection of children's privacy is not a natural or inherent legal given, but rather the outcome of a gradual historical development in international human rights thinking. A foundational milestone in this process is the 1989 United Nations Convention on the Rights of the Child (CRC), which for the first time recognised children as independent subjects of rights, possessing their own dignity, interests, and distinct needs for protection.[1] On the basis of Article 16 of the CRC, children's privacy may be understood as the right to control access to, and the use of, information relating to them, encompassing personal space, private life, and personal data, as well as the safeguarding of their dignity and honour.[2] This approach laid the groundwork for a

1 Warren – Brandeis, The Right to Privacy 193; Palmer, Three Milestones in the History of Privacy 67.

2 Huynh, Protecting children's rights: A comparative analysis between Vietnam and the legal models of the European Union and Hungary 113.

framework of children's rights protection centred on human dignity and the State's protective responsibility, developed largely in a pre-technological context and relying predominantly on passive protective mechanisms rather than proactive tools of technological risk governance.

Vietnam was among the earliest countries to ratify the Convention on the Rights of the Child and has progressively incorporated its normative standards into the domestic legal system. During the pre-digital transformation and early digitalisation phases, Vietnamese legislative thinking on children's privacy largely mirrored the logic of the CRC within a traditional social framework, in which children were primarily situated within family and community relationships, as analysed in previous scholarship by *Huynh Thi Truc Giang*.[3] In this period, children's privacy was predominantly understood as a moral value and a personal right, closely associated with the protection of private life, honour, and dignity in physical spaces and direct social interactions.[4] This approach is reflected in constitutional provisions, civil law, and the Law on Children, which emphasise the protective responsibilities of the family, the State, and society, while paying limited attention to data governance mechanisms or the management of technological risks.

As children's living environments increasingly extend into digital spaces, frameworks for the protection of children's rights that are grounded in traditional social assumptions, particularly the centrality of the family and the moral supervision exercised by parents, have become insufficient to guarantee children's privacy in practice. Empirical studies indicate that parents may themselves constitute common sources of privacy infringement through excessive sharing on social media, thereby generating enduring digital footprints beyond children's effective control. At the same time, existing legal frameworks remain largely oriented towards addressing violations with manifest and tangible consequences, while failing to respond adequately to the structural exploitation of children's data in digital environments.[5]

Against this backdrop, General Comment No. 25 of the United Nations Committee[6] on the Rights of the Child marked a significant shift in the conceptualisation of children's rights protection by affirming, for the first time, States' obligations to ensure the full and effective implementation of the CRC in the digital environment.[7] The General Comment broadened the scope of children's privacy to encompass data processing, algorithmic systems, and automated decision-making, and called for a transition from an ex post, consequence-based approach towards proactive technological risk governance.[8] Under this framework, children's privacy is no longer conceived as a merely defensive right, but as a structural right intrinsically linked to children's autonomy and their holistic development within digital society.

3 Huynh, Protecting children's rights: A comparative analysis between Vietnam and the legal models of the European Union and Hungary 118.

4 Some scholars conceptualise children's privacy as an integral component of human rights, grounded in the principles of human dignity and individual autonomy as articulated in international human rights instruments. This approach emphasises that children's privacy is not merely a derivative moral interest, but a rights-based entitlement warranting autonomous legal protection. See: Pham – Phan, Enhancing the Legal Framework for Protecting the Privacy Rights of Children.

5 Huynh, Safeguarding the Privacy Rights of Children on Social Media Platforms 103.

6 United Nations Committee on The Rights of The Child, General Comment No. 25 on children's rights in relation to the digital environment.

7 Sylwander – Livingstone, The impact of General Comment No. 25 in the Uncrc review process.

8 Ayalew – Verdoodt – Lievens, General Comment No. 25 on children's rights in relation to the digital environment: Implications for children's right to privacy and data protection in Africa.

Vietnam has continued to adopt and internalise this expanded framework for the protection of children's rights amid the acceleration of national digital transformation, as data increasingly constitutes the infrastructure of state governance and social life. The establishment of a national population database, the widespread implementation of personal identification systems[9], and the expansion of online public services[10] have fundamentally reshaped both the scope and intensity of children's data presence in digital environments. At the same time, the digitalisation of education has generated electronic learning records and platform-based learning systems[11], resulting in the large-scale interconnection and utilisation of children's data.

Despite notable progress in strengthening the legal protection of children's personal data and privacy through the incorporation of international standards, Vietnamese law continues to exhibit a degree of legislative lag, particularly in the transition from ethics- and procedure-based models of protection towards frameworks grounded in technological risk management. While a growing body of domestic and international scholarship has examined the limitations of legal protections for children's privacy in both physical and digital contexts[12], much of this literature remains focused on doctrinal analysis or policy effectiveness. Such approaches, though necessary, are insufficient to account for the systemic shortcomings of the existing legal framework. The persistence of regulatory gaps in the face of technological risks reflects not merely a deficit of legal provisions, but deeper constraints in legislative conceptions of privacy, data, and childhood.

Accordingly, an approach grounded in legislative thinking provides a useful analytical lens. In this article, legislative thinking is understood as the constellation of foundational viewpoints, value choices, and models of risk perception that have guided the process of law-making in each historical period. This understanding rests on the premise that legislative activity is not a mere aggregation of discrete decisions, but operates within a relatively stable cognitive framework[13]; at the same time, it reflects a broader socio-cultural system of thought that extends beyond the technical craft of drafting normative legal texts.[14] In this sense, legislative thinking also expresses the manner in which the state identifies and responds to risks within specific historical contexts.[15] It helps elucidate the underlying concepts, perspectives, and policy orientations that have shaped law-making processes across different historical periods. Rather than focusing solely on the substantive content of legal regulation, this approach seeks to explain why legal norms have been formulated in particular ways and to uncover the assumptions that have guided legislative choices. Such an inquiry is essential to

9 Pursuant to Decision No. 06/QĐ-TTg on the development and application of population data, electronic identification, and electronic authentication, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-06-QD-TTg-2022-De-an-phat-trien-ung-dung-du-lieu-ve-dan-cu-2022-2025-499726.aspx?dll=true.

10 Pursuant to Resolution No. 17/NQ-CP on key tasks and solutions for the development of e-Government, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-quyet-17-NQ-CP-2019-nhiem-vu-giai-phap-trong-tam-phat-trien-Chinh-phu-dien-tu-408619.aspx.

11 Pursuant to Decision No. 131/QĐ-TTg on the Digital Transformation Programme in Education and Training, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-131-QD-TTg-2022-Tang-cuong-ung-dung-cong-nghe-thong-tin-trong-giao-duc-501823.aspx.

12 Nguyen – Dang – Bui, Vietnamese Law Regulations Compared to Data Protection 283; Huynh, Safeguarding the Privacy Rights of Children 103; Byrne – Kardefelt – Winther – Livingstone – Stoilova, Global Kids Online.

13 Hall, Policy Paradigms, Social Learning and the State.

14 Silbey, After Legal Consciousness.

15 Luhmann, Risk: A Sociological Theory.

identifying the structural origins of legislative delays and institutional bottlenecks in the protection of children's rights in the face of challenges posed by the digital environment. On this basis, the following section of the article examines the evolution of Vietnamese legislative thinking on children's privacy rights through three representative stages of development, thereby clarifying the law's achievements, limitations, and ongoing challenges in the digital age.

2. The transformation of legislative thinking on children's right to privacy

The development of legislative thinking in Vietnam with respect to privacy rights, particularly children's privacy and personal data protection, has undergone a profound and dynamic evolution. This transformation extends beyond changes in legal terminology and statutory expression, reflecting a deeper shift in the State's normative understanding: from traditional ethical and family-centred conceptions of privacy, to a human rights–based approach, and more recently to a paradigm of digital data governance.

2.1. Pre-digital era: children's privacy as a moral–family value

In the pre-digital transformation period, legislative thinking in Vietnam concerning privacy rights, including children's privacy, was primarily grounded in traditional ethics and family values. This orientation is evident in the 1946[16], 1959[17], and 1980[18] Constitutions, where privacy was framed through the protection of material and relational aspects of family life, such as the inviolability of the home and the confidentiality of correspondence and communications. This approach aligns with a broader historical pattern identified in comparative legal scholarship, according to which early legal systems tended to conceptualise privacy as the protection of family life, residence, and private communications, as reflected in international human rights instruments and common law traditions on privacy. Under this ethical and order-based understanding, privacy was secured largely through social norms and moral expectations within the family and community, rather than through robust legal or institutional mechanisms. Within such a framework, children were not recognised as a distinct rights-bearing group, but were subsumed within the general legal categories of citizens or individuals.

Building on this constitutional foundation, Vietnamese civil law during this period approached the right to privacy primarily through the notion of personal secrets, reflecting a relatively narrow conception of the scope of the right. Article 34(1) of the 1995 Civil Code recognised the

16 Article 11 of the 1946 Constitution provides that *"the home and correspondence of Vietnamese citizens shall not be unlawfully violated",* https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Hien-phap-1946-Viet-Nam-Dan-Chu-Cong-Hoa-36134.aspx.

17 Article 28 of the 1959 Constitution stipulates that *"the law guarantees the inviolability of citizens' homes in the Democratic Republic of Viet Nam, and ensures the confidentiality of correspondence",* https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Hien-phap-1959-Viet-Nam-Dan-Chu-Cong-Hoa-36855.aspx.

18 Article 71 of the 1980 Constitution provides that *"citizens enjoy the right to the inviolability of their domicile. No one may arbitrarily enter another person's home without that person's consent, except in cases permitted by law. Searches of a domicile must be conducted by representatives of competent State authorities in accordance with the law. The confidentiality of correspondence, telephone communications, and telegrams is guaranteed",* https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Hien-phap-1980-Cong-hoa-Xa-hoi-Chu-Nghia-Viet-Nam-36948.aspx.

protection of personal secrets as a personal right of individuals, thereby establishing an initial legal basis for the formal acknowledgment of privacy in Vietnam.[19] This approach and its limited scope were subsequently maintained in the Article 38(1) of 2005 Civil Code.[20] The continued use of the term personal secrets in both codes indicates that legal protection remained largely confined to information and documents regarded as confidential according to prevailing social norms, rather than extending to the broader dimensions of private life, personal living space, or aspects of individual autonomy that may not be inherently secret yet still warrant respect. Notably, this framework displayed little awareness of the distinctive vulnerabilities and needs of children in relation to information and data – an issue that would only become salient with the onset of large-scale digitalisation in Vietnam.

In the context of rapid technological innovation and deepening international integration, Vietnamese legislative thinking has undergone a discernible shift, moving from implicit forms of privacy protection towards the explicit recognition of privacy as an individual and human right.

2.2. Early digital era: from implicit protection to explicit legal recognition

A decisive turning point occurred with the adoption of the 2013 Constitution, in which Article 21[21], for the first time, articulated a comprehensive framework for the protection of privacy. This provision extended constitutional protection beyond physical domains to encompass mental life, personal and family secrets, and multiple forms of private communication. The shift from safeguarding tangible assets, such as the home and correspondence, to protecting the content of private life and individuals' mental space marked a significant expansion of the right to privacy, while simultaneously affirming its close relationship with personal dignity, honour, and reputation. Notably, the inclusion of other forms of private communication reflects a forward-looking constitutional awareness of the evolution of information and communication technologies, thereby laying a constitutional foundation for privacy protection in the digital environment.

This development was further consolidated in the 2015 Civil Code, which represents a significant advancement in the structuring of personal rights under Vietnamese law. In contrast to earlier legislation, Article 38[22]markedly broadened the scope of protection by moving from the

19 Article 34(1) of the 1995 Civil Code provides that *"the right to respect for an individual's private life shall be recognised and protected by law",* https://thuvienphapluat.vn/van-ban/Quyen-dan-su/Bo-luat-Dan-su-1995-44-L-CTN-39391.aspx.

20 Article 38(1) of the 2005 Civil Code provides that "the right to the privacy of an individual shall be respected and protected by law", https://thuvienphapluat.vn/van-ban/Quyen-dan-su/Bo-luat-Dan-su-2005-33-2005-QH11-2463.aspx.

21 Article 21 of the 2013 Constitution provides as follows: *"(1) Everyone has the right to the inviolability of private life, personal secrets, and family secrets, and has the right to protect his or her honour and reputation. Information relating to private life, personal secrets, and family secrets shall be safeguarded by law; (2) Everyone has the right to the confidentiality of correspondence, telephone communications, telegrams, and other forms of private information exchange. No one may unlawfully open, monitor, seize, or otherwise interfere with another person's correspondence, telephone communications, telegrams, or other forms of private information exchange",* https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Hien-phap-nam-2013-215627.aspx.

22 Article 38 of the 2015 Civil Code provides that: *"(1) Private life, personal secrets, and family secrets are inviolable and shall be protected by law; (2) The collection, storage, use, or disclosure of information relating to an individual's private life or personal secrets requires that individual's consent; the collection, storage, use, or disclosure of information relating to family secrets requires the consent of the family*

notion of secrets of private life to the more comprehensive formulation of private life, personal secrets, and family secrets. This shift reflects a more nuanced understanding of the multidimensional nature of private life and underscores the importance of protecting individuals' control over information within civil and commercial relationships. Notably, the 2015 Civil Code was the first to recognise the principle of confidentiality of private information between contracting parties, signalling a transition from a purely defensive conception of privacy towards one that also regulates conduct within economic and social transactions. These developments draw on international legal experience while responding to the internal demands of Vietnamese society amid rapid and widespread technological change.

Building on this legal foundation, the 2016 Law on Children marked a fundamental shift in Vietnamese legislative thinking by, for the first time, treating children's private life as an independent category requiring a higher level of protection than that afforded to adults. Article 21[23] of this code affirms children's inviolable rights to privacy, personal secrets, and family secrets, while simultaneously introducing a dual-consent requirement for the disclosure or publication of children's information and images. The Law also enshrines the principle of the best interests of the child as a guiding standard for all related decisions and interventions. Subsequent implementing instruments, particularly Decree No. 56/2017/ND-CP[24], significantly clarified the scope of children's private life by enumerating categories of protected information, including personal identification data, health and education records, and sensitive information relating to violence, abuse, or legal violations. The Decree further imposes legal obligations on agencies and organisations concerning confidentiality, purpose limitation, and the adoption of technical measures to prevent data breaches. These protections were further strengthened by Decree No. 130/2021/ND-CP[25], which specifies acts constituting violations and prescribes concrete sanctions, thereby affirming that infringements of children's privacy are no longer viewed merely as moral transgressions but as serious legal violations subject to strict enforcement.

members concerned, unless otherwise provided by law; (3) An individual's correspondence, telephone communications, telegrams, electronic databases, and other forms of private information exchange shall be safeguarded in terms of security and confidentiality. The opening, monitoring, or seizure of correspondence, telephone communications, telegrams, electronic databases, or other forms of private information exchange of another person may only be carried out in cases prescribed by law; (4) Parties to a contract shall not disclose information relating to each other's private life, personal secrets, or family secrets that they have become aware of in the course of the formation or performance of the contract, unless otherwise agreed", https://thuvienphapluat.vn/van-ban/Quyen-dan-su/Bo-luat-dan-su-2015-296215.aspx.

23 Article 21 of the 2016 Law on Children provides as follows: *"(1) Children enjoy the inviolable right to privacy, including personal privacy and family secrets, in accordance with the best interests of the child; (2) Children are protected by law in respect of their honour, dignity and reputation, as well as the confidentiality of correspondence, telephone communications, telegrams, and other forms of private information exchange; they are also safeguarded against any unlawful interference with their private information"*, https://thuvienphapluat.vn/van-ban/Giao-duc/Luat-tre-em-2016-303313.aspx.

24 Decree No. 56/2017/NĐ-CP, issued on 9 May 2017, provides detailed guidance for the implementation of the 2016 Law on Children, https://thuvienphapluat.vn/van-ban/Van-hoa-Xa-hoi/Nghi-dinh-56-2017-ND-CP-huong-dan-Luat-tre-em-340397.aspx.

25 Decree No. 130/2021/NĐ-CP, issued on 30 December 2021, regulates administrative sanctions for violations in the fields of social assistance, social protection, and child welfare, https://thuvienphapluat.vn/van-ban/Vi-pham-hanh-chinh/Nghi-dinh-130-2021-ND-CP-xu-phat-vi-pham-hanh-chinh-bao-tro-xa-hoi-va-tre-em-499523.aspx.

Overall, the period from 2013 to 2016 marked a profound transformation in Vietnam's legislative thinking, characterised by a shift from locating privacy within a traditional ethical framework to formally recognising and codifying privacy – particularly children's privacy – as an integral component of the human rights system. This transition laid a critical foundation for Vietnamese law to enter the era of digital data governance, in which privacy is understood not merely as a right to be respected in principle, but as one that must be actively safeguarded through proactive, modern mechanisms of information control and personal data protection.

2.3. Digital transformation era: children's privacy as digital data protection

As data has become a central resource in economic and social life, Vietnamese legislative thinking has entered a new phase in which children's privacy rights are increasingly conceptualised as a form of personal data protection within the digital environment. This shift in legislative thinking is clearly reflected in a range of key national legal instruments adopted during Vietnam's digital transformation period.

Decree No. 13/2023/ND-CP[26], for the first time, introduced a legally binding definition of personal data and drew a distinction between basic and sensitive data, thereby laying the conceptual groundwork for recognising children's data as a specific category requiring enhanced protection mechanisms. Subsequently, the 2025 Law on Personal Data Protection[27] marked a significant advancement at the statutory level by affirming the intrinsic link between personal data and the right to privacy, and by positioning data protection as the most effective means of safeguarding that right in a context where individual identities are increasingly constituted through digital footprints. The Law establishes a comprehensive framework of data subject rights, including consent, withdrawal of consent, access, and erasure, while strictly prohibiting the purchase, sale, or unlawful disclosure of personal data. It also introduces a notable shift in enforcement by providing for administrative fines of up to 5 per cent of annual revenue for violations involving cross-border data transfers. These provisions compel enterprises to make substantive investments in data governance, although their implementation may give rise to regulatory overlap with sector-specific regimes, such as those governing information technology, telecommunications, and healthcare.

Overall, the digital transformation period represents a critical turning point in Vietnam's legislative thinking on children's privacy rights, as these rights have been reconceptualised as a core component of personal data protection, particularly with respect to children's sensitive data. Legislative protection has shifted from a predominantly ethics-based model towards an integrated framework combining legal, technical, and data governance mechanisms. Within this framework, children are increasingly recognised as a high-risk data group, necessitating stricter, more transparent, and more robust standards of control and accountability. As a result, children's privacy rights no longer operate as a stand-alone legal entitlement but have become a central pillar of the national data governance architecture.

26 Decree No. 13/2023/ND-CP, issued on 17 April 2023, regulates the protection of personal data, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx.

27 Law No. 91/2025/QH15, adopted on 26 June 2025, governs the protection of personal data and entered into force on 1 January 2026, https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-Bao-ve-du-lieu-ca-nhan-2025-so-91-2025-QH15-625628.aspx.

3. Gaps in contemporary legislative thinking that undermine the protection of children's privacy in the digital age

Although Vietnam has achieved notable institutional progress through the adoption of the 2025 Law on Personal Data Protection and its accession to the Hanoi Convention[28] in the same year, thereby strengthening the legal framework for data protection and the prevention of cybercrime in general, and for children in particular, practical implementation reveals that legislative thinking continues to lag behind the pace of technological development. In particular, existing legal approaches have yet to engage systematically with concrete technical solutions capable of addressing the operational realities of data-driven and AI-enabled environments.

First, legislative thinking continues to place disproportionate emphasis on ex post responses to harm rather than on proactive risk management at the technology design stage. Existing regulations are largely structured to sanction violations after they have occurred, such as the unlawful disclosure of private information or defamation, rather than to require digital platforms to prevent privacy risks from the outset. A salient example can be found in free educational gaming applications, which are able to collect data on children's reaction times and behavioural patterns in order to optimise user-retention algorithms. Empirical studies demonstrate that children in digital environments are increasingly datafied and rendered as algorithmic subjects, whose interactions and habitual behaviours are continuously monitored and exploited to shape platform architectures in the interests of powerful commercial actors.[29] Although such practices may not entail the external disclosure of information and therefore often fall outside the scope of existing privacy rules, they nonetheless involve the intensive commercial exploitation of children's behavioural data. Current legal frameworks remain insufficient to compel service providers to implement default no-tracking or privacy-by-design settings at the product development stage, thereby leaving children structurally exposed to algorithmic practices that capitalise on their behavioural data.

Second, regulatory thinking remains overly reliant on formal administrative procedures, often at the expense of empowering individuals through effective technical control mechanisms. Although the enactment of the 2025 Law on Personal Data Protection, particularly its requirement for parental consent, represents a commendable legislative initiative, this approach continues to rest on an unrealistic assumption: that complex technical challenges can be adequately addressed through relatively simple procedural or documentary requirements.

28 The Hanoi Convention, the commonly used name for the United Nations Convention on Countering Cybercrime, was adopted by the United Nations General Assembly on 24 December 2024 and opened for signature in Hanoi on 25 October 2025, with the participation of 72 signatory States. The Convention aims to prevent and combat high-technology crime, particularly transnational cybercrime, https://baochinhphu.vn/tong-quan-cong-uoc-ha-noi-noi-dung-chinh-cau-truc-va-pham-vi-ap-dung-102251025173814819.htm.

29 Livingstone – Third, Children and young people's rights in the digital age: An emerging agenda 655.

This mismatch is evident in at least three respects. First, at the level of enforcement, digital platforms typically adopt only rudimentary technical solutions[30], most commonly a confirmation dialogue stating 'I am a parent and I agree.' While such mechanisms may formally satisfy statutory consent requirements, they are functionally ineffective in practice[31], as children can readily self-confirm consent without parental knowledge or involvement.[32] As a result, legal safeguards are inadvertently reduced to a purely formal, checkbox-based procedure. Second, in terms of regulatory instruments, existing legislation lacks binding requirements for minimum technical standards. In particular, it does not mandate the adoption of robust authentication or verification tools, such as age-appropriate identity verification technologies, secondary device authentication involving parents, or easily accessible mechanisms for data erasure. It is precisely this absence of enforceable technical safeguards that renders legally mandated parental consent largely ineffective in practice, undermining its capacity to provide meaningful protection for children in digital environments.

Moreover, legislative thinking grounded primarily in the parental consent model is increasingly ill-suited to digital environments characterised by the emergence of so-called algorithmic parenting. As noted by *Lin* and *Wu* (2024)[33], recommendation systems and hyper-nudge technologies are progressively displacing traditional parental roles by shaping children's behaviour, attention, and decision-making, thereby establishing a de facto guardianship relationship between digital platforms and children. In this context, parents often lack both the awareness and the technical capacity to counteract the subtle and continuous influence exerted by algorithmic systems. Consequently, consent-based regulatory approaches risk becoming largely ineffective unless they are complemented by direct regulatory intervention in algorithm design and deployment from the outset.

The limitations of this predominantly managerial approach are clearly illustrated by empirical data from the 2023 Child Online Safety Index (COSI)[34], a global metric designed to assess the effectiveness of child protection mechanisms across nations.[35] COSI evaluates national performance not merely based on the existence of laws, but through a holistic assessment of six critical stakeholders: (1) Children's cyber competencies; (2) Family support and guidance; (3) Digital citizenship education in schools; (4) The accountability of Ict companies; (5) Government policies; and (6) Technological infrastructure.

Comparative data reveals a significant disparity in outcomes. While jurisdictions that have successfully integrated strict technical standards with models of social co-governance- most notably China and Singapore-achieved the highest tier of online safety (Rank A, or Level 4/4), Vietnam remained at a moderate level (Rank B, or Level 3/4). Notably, China achieved maximum scores across relevant indicators, reflecting the effectiveness of a strategy that combines legal mandates with rigorous technical enforcement. This gap suggests that, notwithstanding considerable efforts to develop legal frameworks, prevailing legislative thinking in Vietnam has yet to foster a sufficiently robust and coherent protective ecosystem. The current reliance on administrative compliance has failed to generate the synergistic impact seen in neighbouring jurisdictions, where responsibility is more effectively distributed across the six pillars of the digital safety ecosystem (Figure 1).

30 Massa [et al.], Digital technologies and knowledge processes 2.

31 Oecd, The Digital Transformation of Smes 17.

32 Hsu – Chen, Analyzing the mechanisms by which digital platforms 2.

33 Wu – Lin, Algorithmic Regulation for the Protection of Children 8.

34 Dq Institute, Impact Measure 2023.

35 Niyu – Purba, E-Safety 130.

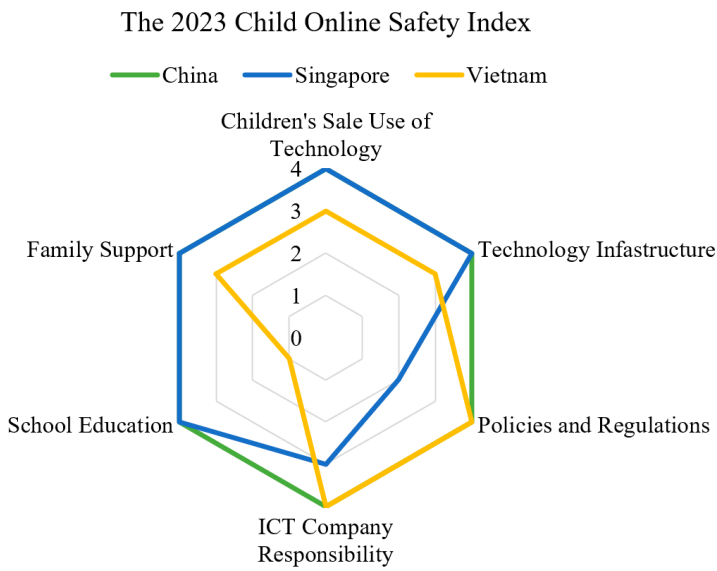

Figure 1: *The 2023 Child Online Safety Index (COSI) comparison. Vietnam (Rank B) lags behind Singapore and China (Rank A) in overall safety scores. Source: DQ Institute*[36]

Third, insufficient awareness of emerging forms of high-technology abuse has left existing legal frameworks ill-equipped to address non-traditional risks to children. The rapid proliferation of deepfake technologies provides a particularly stark illustration. Empirical research indicates that approximately 96 per cent of online deepfake content involves non-consensual pornographic material, and that in South Korea alone, nearly 200 cases in 2024 directly targeted school-aged children.[37] By contrast, Vietnamese law currently lacks specific provisions to define, prevent, or sanction such conduct, instead relying on general rules relating to the protection of honour and dignity. This legislative approach fails to recognise that the extraction of children's facial images from ordinary photographs and their use in the creation of sexually explicit deepfake content constitutes not merely an affront to reputation, but a distinct form of digital sexual abuse. The absence of a tailored legal response creates a significant regulatory blind spot, exposing children to heightened risks of cyber-enabled exploitation and abuse.

Fourth, legislative thinking remains largely confined to territorial notions of state authority and geographical jurisdiction, rather than adapting flexibly to the realities of cross-border data flows. Although Vietnam's accession to the Hanoi Convention in 2025[38] represented an important diplomatic and institutional milestone, this framework is primarily effective within the sphere of criminal justice and serious offences, leaving substantial regulatory gaps in relation to administrative and civil violations such as online bullying and privacy infringements. A particularly pressing challenge arises from the fact that, even where legislation requires cross-border digital platforms to locate servers within Vietnam in the name of data sovereignty, effective control over encrypted data and content moderation remains embedded within the internal governance structures of parent

36 Dq Institute, Impact Measure 2023.

37 Nguyen – Le – Phan, Vietnamese law on personal data protection 137.

38 Vietnam Government Portal, Overview of the Hanoi Convention.

companies based abroad. This limits the capacity of domestic authorities to intervene promptly to remove harmful content. Moreover, delays inherent in mutual legal assistance procedures – despite the existence of 24/7 contact mechanisms – are fundamentally mismatched with the rapid circulation of harmful digital material.[39] While a single abusive video may irreparably damage a child's reputation within hours, legal processes may require weeks to initiate a response. Digital platforms frequently invoke conflicts between data-sharing obligations and the stringent privacy laws of host jurisdictions to justify non-cooperation or delay, thereby exposing the limitations of territorially based governance in the face of a globalised digital environment.

Fifth, legislative thinking continues to exhibit a tendency to treat children as a homogeneous category, rather than differentiating levels of protection according to age-related[40] psychophysiological development.[41] A significant limitation lies in the prevailing approach of grouping all children under a single age threshold – commonly under 16 – thereby applying uniform protection mechanisms without adequately accounting for their distinct privacy needs. For instance, a 15-year-old seeking confidential online psychological counselling may encounter substantial barriers if legal rules rigidly impose parental consent and supervision across all digital services. This absence of stratified, child-sensitive regulatory thinking results in one-size-fits-all rules that simultaneously fail to provide sufficient safeguards for younger children while unnecessarily restricting older children's autonomy, access to information, and legitimate expectations of private space essential to their independent development.

Accordingly, while the enactment of the 2025 Law on Personal Data Protection constitutes a necessary institutional foundation, it is not, in itself, sufficient to ensure effective protection of children in the digital age. Achieving this objective requires a more profound shift in legislative thinking – from reliance on administrative and procedural control towards a risk-based regulatory approach grounded in enforceable technical standards and substantive, multi-stakeholder cooperation.

4. Proposed directions for legal reform to strengthen children's right to privacy in the digital age

Confronted with systemic challenges in both legislative thinking and the practical protection of children's privacy, Vietnam requires a fundamental reorientation of its lawmaking strategy. Rather than confining itself to the enactment of prohibitive norms, the law must assume a constructive role in shaping a safe digital ecosystem in which children's rights are secured through the combined deployment of legal instruments and technological solutions. Drawing on international experience and an assessment of domestic conditions, this article advances four principal groups of reform proposals. First, legislative thinking should be reoriented towards a child-centred, design-based regulatory model. This represents the most fundamental response to the structural drivers of excessive data collection. Rather than relying primarily on ex post consent mechanisms, the law should internalise privacy protection at the design stage and establish privacy-by-default as a mandatory standard for all digital products and services likely to be accessed by children. Digital platforms should therefore be under a legal obligation to apply the highest level of protection to accounts identified as belonging to children from the moment of activation, irrespective of parental consent, which in practice often operates as a purely formal safeguard. In concrete terms, the Law

39 Romero Moreno, Generative AI and deepfakes 297.

40 Weithorn, A constitutional jurisprudence of children's vulnerability 194.

41 Steinberg – Icenogle, Using developmental science to distinguish adolescents and adults 33.

on Personal Data Protection and its implementing instruments should prohibit default location tracking, behavioural data collection, and targeted advertising for users under the age of sixteen. Data-sharing functions should be disabled by default and activated only through informed and proactive intervention by a guardian. Comparative experience offers clear guidance in this respect. The United Kingdom's Age-Appropriate Design Code (the Children's Code), widely regarded as a global benchmark, requires online services, such as social media platforms, games, and applications, to configure the highest privacy settings by default for child users.[42] Features including geolocation and profiling must be switched off unless a compelling justification exists and active steps are taken to enable them.[43] In parallel, mandatory child-focused data protection impact assessments should be imposed on large technology companies prior to the deployment of new products or services, in order to identify and mitigate risks at the earliest, conceptual stage of technological development.[44]

Second, a co-governance framework grounded in a gatekeeper principle should be established. To move beyond the limitations of a purely administrative and state-centric regulatory mindset, Vietnam can draw valuable lessons from models of social co-governance adopted in jurisdictions such as China and Singapore, where responsibility for protecting children in digital environments is shared among the State, digital service providers, and society at large. In particular, for cross-border platforms that control vast volumes of children's data, regulatory thinking should shift from a logic of limited or conditional liability towards a gatekeeper model imposing a duty of maximum effort. Under this approach, digital platforms would bear clearly defined obligations not only to remove harmful content upon notification, but also to proactively assess, prevent, and mitigate risks arising from addictive algorithmic design and the commercial exploitation of children's data. To ensure accountability, platforms should be required to publish regular, transparent reports detailing their data processing practices relating to children and the effectiveness of the protective measures they have implemented. At the same time, serious infringements involving children's data should attract sanctions calculated as a proportion of global turnover, thereby replacing fixed administrative fines that are insufficient to deter violations by large technology corporations.

Revenue-based and progressive penalty regimes designed to generate genuine deterrent effects on large technology corporations have been adopted across several major jurisdictions, including Vietnam, China, and the European Union. In Vietnam, Clause 4 of Article 8 of the 2025 Law on Personal Data Protection represents a significant enforcement innovation by providing for administrative fines of up to 5 per cent of revenue for serious violations, notably those involving unlawful cross-border data transfers. In China, the Regulations on the Protection of Minors in Cyberspace, enacted in 2023, authorise penalties of up to RMB 1 million or, where illicit gains exceed that threshold, up to ten times the amount of illegal profit.[45] At the European level, the General Data Protection Regulation (GDPR)[46] stands as a pioneering regulatory framework, establishing stringent, turnover-based sanctions aimed at safeguarding personal data and compelling corporate compliance with demanding data processing standards.[47]

42 Elvy, Age-Appropriate Design Code Mandates 1030.

43 Wu – Lin, Algorithmic Regulation for the Protection of Children 5.

44 Grace – Abel – Salen, Child-Centered Design in the Digital World 293.

45 Liza – Tianyun, China Releases Regulation on the Protection of Children.

46 This European Union regulation, in force since 2018, safeguards the privacy and personal data of EU citizens and requires organisations to comply with stringent rules on data security and data processing.

47 Nguyen – Le – Phan, Vietnamese law on personal data protection 135.

Third, the construction and legal recognition of digital literacy as a protected right are of critical importance. Acknowledging that technical safeguards alone cannot address all risks, equipping children and parents with a form of digital immunity represents the most sustainable long-term strategy. Legislative thinking should therefore treat digital literacy not merely as a promotional or awareness-raising initiative, but as a mandatory and enforceable component of the national education framework. Core competencies relating to data privacy, the identification of online fraud and manipulation, and practical self-protection skills should be systematically integrated into the formal curriculum from primary education onwards. In parallel, targeted programmes should be developed to enhance parents' digital capacity, enabling them to function as an effective first line of defence for their children rather than relying exclusively on platform-provided control tools. Over time, a digitally literate society can generate bottom-up regulatory pressure, compelling businesses to comply with higher ethical and legal standards in the processing of children's data.

A prominent illustration of this approach can be found in Finland, which is widely regarded as one of the most successful countries in addressing misinformation and digital risks through education. Within the Finnish legal and policy framework, media literacy is recognised as a core civic competence. Digital and media literacy education is legally embedded and mandatorily integrated into the national curriculum from early childhood and primary education onwards. Rather than being taught as a stand-alone subject, these competencies are systematically incorporated across disciplines, including mathematics (for example, understanding how statistical data may be manipulated), art (analysing the alteration and manipulation of images), and history (examining the mechanisms and historical patterns of misinformation). This cross-curricular approach enables children to develop the capacity to identify deepfake content, digital fraud, and other forms of online manipulation organically[48], reducing reliance on constant technical intervention.[49]

Fourth, strengthening digital justice mechanisms and advancing substantive international cooperation are essential to addressing the challenges posed by territorial boundaries in the digital environment. To overcome jurisdictional constraints, Vietnam should maximise the potential of the Hanoi Convention and existing mutual legal assistance arrangements by establishing transnational rapid-response channels dedicated to the protection of children online. This approach would benefit from the creation of a specialised national authority or focal point for child online safety, vested with sufficient legal powers to require the prompt removal of content infringing children's privacy rights without resorting to protracted judicial procedures. Such an authority could also act on behalf of Vietnamese children in lodging complaints and pursuing compensation claims against cross-border digital platforms. In parallel, the development of bilateral and multilateral agreements on data sharing, as well as the mutual recognition of administrative sanctions in the field of data protection, is crucial to ensuring that violations of children's rights do not escape accountability through jurisdictional loopholes.

A leading example of such an institutional model is Australia's eSafety Commissioner[50], the world's first specialised government authority dedicated to online safety. Established with extensive statutory powers, the eSafety Commissioner is authorised to require digital platforms to remove cyberbullying material or abusive imagery involving children within a strict 24-hour timeframe.[51] In cases of non-compliance, the agency may impose substantial administrative

48 Horn – Veermans, Critical thinking efficacy and transfer skills 31.

49 Du, Finland teaches how to fight fake news from kindergarten.

50 Australian Government, Australia eSafety Women Program 2021.

51 Martin, Online safety regulation 29.

penalties of up to Aud 600.000 per violation[52] and, where necessary, order the restriction or suspension of access to non-compliant services within Australian territory. This enforcement model demonstrates how a specialised, well-empowered regulatory body can deliver rapid and effective protection for children's rights in digital environments.

Enhancing the legal framework requires more than incremental amendments to statutory language; it calls for a fundamental transformation in governance thinking. By integrating hard regulatory and technical measures – such as privacy by design and by default – with softer, socially embedded approaches, including comprehensive digital literacy education, and coupling these with flexible yet robust enforcement mechanisms, Vietnam can construct a resilient legal architecture capable of protecting future generations from the pervasive data-driven dynamics of the digital age.

5. Conclusion

Children's privacy in the digital age can no longer be understood solely as a matter of social ethics or the protection of personal honour; it has evolved into a complex challenge of data governance shaped by technological infrastructures, algorithmic systems, and platform power. Through an analysis of the evolution of legislative thinking in Vietnam, this article demonstrates that the legal protection of children's privacy follows a clear trajectory of normative awareness – from family-based moral values, to the recognition of privacy as an individual and human right, and ultimately to its reconceptualisation as the right to personal data protection in digital environments. This progression reflects the State's sustained efforts to adapt legal frameworks to the realities of digital transformation, while underscoring the increasingly central role of data in constituting children's identities and private lives. However, the article also demonstrates that institutional advancements have not been fully matched by corresponding innovation in legislative thinking. The continued reliance on ex post regulatory responses, formalistic consent procedures, and the absence of mandatory technical safeguards at the design stage have significantly undermined the practical effectiveness of children's privacy protection. In the face of emerging threats such as behavioural data exploitation, algorithmic manipulation, and the growing prevalence of deepfake technologies, this approach reveals its increasingly outdated character when measured against the operational realities of contemporary digital environments.

On the basis of these analyses, this article argues that strengthening the legal protection of children's privacy in the digital age cannot be achieved merely through the incremental addition of regulatory provisions. Rather, it requires a fundamental transformation in legislative thinking. The law must assume a constructive role by obliging technology actors to identify and manage risks at the design stage, while simultaneously integrating enforceable technical standards, co-governance mechanisms, and enhanced digital literacy for both children and families. Only through such a paradigm shift can children's privacy be protected in a genuinely proactive, effective, and sustainable manner in the face of the increasingly complex challenges posed by data-driven technologies and artificial intelligence.

52 Hollingworth, X/Twitter fined over $600,000.

Sources and literature

Australian government: Australia eSafety Women Program 2021, https://www.pmc.gov.au/sites/default/files/submissions/submission-95-australias-esafety-commissioner.pdf (12. 12. 2021)

Ayalew, Y. E. – Verdoodt, V. – Lievens, E.: General Comment No. 25 on children's rights in relation to the digital environment: Implications for children's right to privacy and data protection in Africa. Human Rights Law Review 2024, https://doi.org/10.1093/hrlr/ngae018 (01. 01. 2026)

Byrne, Jasmina – Kardefelt – Winther, Daniel – Livingstone, Sonia – Stoilova, Mariya: Global kids online: research synthesis 2015–2016. Unicef – London School of Economics and Political Science 2016

Dq Institute: Impact Measure (COSI) 2023, https://www.dqinstitute.org/impact-measure/ (12. 10. 2023)

Du, Lam: Finland teaches how to fight fake news from kindergarten. Vietnamnet 2023, https://vietnamnet.vn/phan-lan-day-chong-tin-gia-tu-mau-giao-i5013144.html (01. 01. 2026)

Dung, T. T. T. – Duong, V.N.: Policy recommendations for enhancing children's personal data protection: A case study in Vietnam. Environment 2025, 8–9.

Elvy, Stacy-Ann: Age-Appropriate Design Code Mandates. University of Pennsylvania Journal of International Law, Vol. 45/2024, 953–1054.

Grace, Thomas D. – Abel, Christie – Salen, Katie: Child-Centered Design in the Digital World: Investigating the Implications of the Age-Appropriate Design Code for Interactive Digital Media. In: Interaction Design and Children. New York 2023, 289–297.

Hall, Peter A.: Policy paradigms, social learning and the state: The case of economic policymaking in Britain. Comparative Politics (3) Vol. 25/1993, 275–296.

Hollingworth, David: X/Twitter fined over $600,000 by Australia's eSafety Commissioner. Cyber Daily 2023, https://www.cyberdaily.au/culture/9680-x-twitter-fined-over-600-000-by-australia-s-esafety-commissioner (01. 01. 2026)

Horn, Shane – Veermans, Koen: Critical thinking efficacy and transfer skills defend against 'fake news' at an international school in Finland. Journal of Research in International Education, No. 1/2019, 31.

Hsu, Pi-Chun – Chen, Ru-Si: Analyzing the mechanisms by which digital platforms influence family-school partnerships among parents of young children. Sustainability, Vol. 15/2023, 16708.

Huynh Thi Truc, Giang: Safeguarding the Privacy Rights of Children on Social Media Platforms. Jura No. 4/2023, 103–120.

International Commission of Jurists: The right of privacy and rights of the personality. International Commission of Jurists Review, No. 1/1967, 9–27.

Livingstone, Sonia – Stoilova, Mariya – Nandagiri, Ranjana: Children's Data and Privacy Online: Growing Up in a Digital Age (Evidence Review). London School of Economics and Political Science, London 2019, https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf (07. 12. 2025)

Livingstone, Sonia – Third, Amanda: Children and young people's rights in the digital age: An emerging agenda. New media & society, 2017, 19.5: 657–670.

Liza, Mark – Tianyun: China Releases Regulation on the Protection of Children in Cyberspace. Haynes Boone 2024, https://www.haynesboone.com/news/alerts/china-releases-regulation-on-the-protection-of-children-in-cyberspace (12. 12. 2025)

Luhmann, Niklas: Risk: A sociological theory. London – New York 2017

Martin, Noelle: Online safety regulation of deepfake abuse: a case study on Australia's eSafety Commissioner. Griffith Law Review, No. 1/2025, 29.

Massa, Silvia [et al.]: Digital technologies and knowledge processes: new emerging strategies in international business. A systematic literature review. Journal of Knowledge Management, Vol. 27/2023, 330–387.

Nguyen Thi Truc, Mai – Le Minh, Hai – Phan Khanh, Chi.: Vietnamese law on personal data protection in the digital age under the impact of deepfake technology. Law and Practice Journal, Vol. 60/2024, 135.

Nguyen Vu Tram, Anh – Dang Thi Thuy, An – Bui Thi Cam, Tu: Vietnamese Law Regulations Compared to Data Protection and Privacy Acts in Other Countries. In: The International Conference on Economics, Law and Government 2024, 283.

Niyu, Niyu – Purba, Herman: E-Safety: Keamanan Di Dunia Maya Bagi Pendidik Dan Anak Didik. Prosiding Konferensi Nasional Pengabdian Kepada Masyarakat Dan Corporate Social Responsibility, Vol. 4/2021, 729–737.

Oecd: The Digital Transformation of Smes. Oecd Studies on Smes and Entrepreneurship. Paris 2021

Palmer, Vernon Valentine: Three milestones in the history of privacy in the United States. Journal of Civil Law Studies, No. 1/2011, 149–178.

Phạm, Thị Duyên Thảo – Phan, Thị Lan Phương. "Hoàn thiện pháp luật về bảo vệ quyền riêng tư của trẻ em", http://www.lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid=210643 (07. 12. 2025)

Romero Moreno, Felipe: Generative AI and deepfakes: a human rights approach to tackling harmful content. International Review of Law, Computers & Technology, (3) Vol. 38/2024, 297–326.

Silbey, Susan S.: After legal consciousness. Annual Review of Law and Social Science, No. 1/2005, 323–368.

Soni, Nibtin: Digital Footprints of the Young: Privacy Concerns and Awareness among Teen Social Media Users. ResearchGate 2024, https://www.researchgate.net/publication/387476950_Digital_footprints_of_the_young_privacy_concerns_and_awareness_among_teen_social_media_users (07. 12. 2025)

Steinberg, Laurence – Icenogle, Grace: Using developmental science to distinguish adolescents and adults under the law. Annual Review of Developmental Psychology, 2019, 1.1: 21–40.

Sylwander, K. R. – Livingstone, S.: The impact of General Comment No. 25 in the Uncrc review process. Digital Futures for Children, London School of Economics and Political Science 2025

United Nations: E-Government Survey 2022: The Future of Digital Government. United Nations Department of Economic and Social Affairs. New York 2022, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022 (07. 12. 2025)

Vietnam Government Portal: Overview of the Hanoi Convention: Main contents, structure and scope of application, https://baochinhphu.vn/tong-quan-cong-uoc-ha-noi-noi-dung-chinh-cau-truc-Ava-pham-vi-ap-dung-102251025173814819.htm (07. 12. 2025)

Warren, Samuel D. – Brandeis, Louis D.: The right to privacy. Harvard Law Review, Vo. 5/1890, 193–220.

Weithorn, Lois A: A constitutional jurisprudence of children's vulnerability. Hastings LJ, 2017, 69: 179.

Wu, Hong – Lin, Huanming: Algorithmic Regulation for the Protection of Children. Ssrn 2024