West Science Law and Human Rights
Vol. 3, No. 03, July 2025, pp. 265~273

Digital Education and the Challenge of Personal Data Protection: An International Human Rights Law Perspective on State Obligations

Vania Sokya Fausta[1], Rina Arum Prastyanti[2]
[1,2]Duta Bangsa University

Article Info

Article history:

Received June, 2025
Revised July, 2025
Accepted July, 2025

Keywords:

Person Data Protection
Human Rights
Digital Education
Due Diligence
State Obligations

ABSTRACT

There is currently a conflict between technological innovation and the preservation of privacy rights as a result of the increasing collection of students' personal data caused by the digital transformation of education. Through the lens of international human rights law, this research seeks to understand states' obligations to protect personal data in the context of digital education. This research examines three theoretical frameworks: the concept of International Due Dilligence, the interpretation of General Comment No. 16 of the UN Human Rights Committee, and Human Rights Protection Theory, using a normative legal methodology and doctrinal approach. The findings demonstrate significant weaknesses in traditional regulatory frameworks that prevent education data protection from incorporating a human rights perspective. In the context of digital education, this research shows that the state has three duties to uphold, defend and fulfill the right to data privacy. To assess the state's compliance with its duties to prevent, address and remedy education data privacy violations, this research creates an evaluative model based on due diligence. The results are important for creating a human rights-based approach to regulating education data, providing a conceptual framework that strikes a balance between protecting fundamental rights and technological advancement, and increasing state accountability in digital education data governance.

Corresponding Author:

Name: Rina Arum Prastyanti
Institution Address: Jl. Ki Mangun Sarkoro No. 20, Nusukan, Banjarsari, Surakarta, Indonesia
e-mail: rina_arum@udb.ac.id

1. INTRODUCTION

The digital era has brought tremendous transformation to the education sector, especially after the COVID-19 pandemic accelerated the adoption of online learning globally. The digital education system now relies heavily on massive data collection and processing, which includes personal identity information, academic records, learning patterns, and biometric data. This process involves various stakeholders, ranging from educational institutions, goverments, to multinational education technology companies. However, this situation also presents significant challenges related to personal data protection, which has a direct impact on fundamental human rights, particularly the right to privacy.

The academic discourse on data protection in the context of digital education has evolved in various directions. Livingstone and Third (2017) highlighted the vulnerability of children and young people in the digital education ecosystem, while Bennet and Raab (2020) identified the gap between traditional data protection regulation and the current reality of educational technology. Kerber's (2016) research shows that regulations that focus solely on consent are becoming increasingly inadequate in the context of complex and unbalanced data collection in education systems. In addition, Selwyn (2019) highlights the tension between optimizing data-driven learning and the ethical demands of protecting learners' autonomy and privacy.

While these studies make important contributions, there is a conceptual gap in integrating international human rights law perspectives into the analysis of data protection in education. Most previous studies tend to focus on the technical aspects of regulation or the ethical dimension, but do not comprehensively link it to the normative framework of human rights implications of the "datafication" of education, but have not explored in depth how international human rights instruments, such as General Comment No. 16, can be operationalized in this context. Similarly, van der Hof (2017) touches on the due diligence aspect of protecting children's data in the digital ecosystem, but does not develop an analytical framework to evaluate state obligations based on this principle.

A major limitation of previous studies lies in the lack of systematic analysis of how the human rights paradigm, particularly through the lens of Human Rights Protection Theory, can provide a coherent conceptual framework for understanding and evaluating states' obligations to protect personal data in digital education environments. Previous research has also not sufficiently explored the relevance of General Comment No. 16 and the International Due Diligence principle - which has evolved in the broader human rights context - to the specific issues of data protection in education.

This study seeks to bridge that gap by aiming to: (1) conceptualize the protection of personal data in digital education as an integral component of the state's human rights obligations; (2) develop a contemporary interpretive framework of General Comment No. 16 that is responsive to the realities of educational technology; and (3) formulate an evaluative model based on the principles of International Due Diligence to measure and enhance state accountability in education data protection.

The significance and novelty of this research lies in the interdisciplinary approach that links international human rights jurisprudence with data protection issues in the context of digital education. From a theoretical perspective, this research expands the understanding of the concept and scope of state obligations in the digital era, especially in the field of education. Practically, this research provides a useful analytical framework for policy makers, educational institutions and other stakeholders to design and evaluate data protection systems that are in line with international human rights standards. Thus, this research not only contributes to the academic discourse around human rights law in the digital era, but also supports practical efforts in balancing educational technology innovation with the protection of individual fundamental rights.

2. LITERATURE REVIEW

2.1 Livingstone and Third (2017)

Livingstone and Third (2017) argued that children and young people are among the most vulnerable groups in the digital education ecosystem due to the lack of adequate data protection measures. They emphasized the need for a child-rights-based approach when designing education technology policies (Livingstone & Third, 2017: 659). However, their study did not explore the legal implications under international human rights law.

2.2 Kerber (2016)

Kerber (2016) highlighted that consent-based data protection mechanisms are

increasingly inadequate in modern digital education systems, where data collection is often complex and imbalanced. He stressed the need for a stronger structural approach to safeguard the right to privacy (Kerber, 2016). Nevertheless, his analysis did not directly connect with state obligations under international human rights instruments.

2.3 Van der Hof (2017)

Van der Hof (2017) discussed children's data protection in the digital world and acknowledged the importance of the due diligence principle. She pointed out that states must exercise due diligence in protecting children's personal data, but did not develop a systematic evaluative framework to assess state compliance with this principle (van der Hof, 2017). This research attempts to address that gap by constructing an evaluative model based on international human rights law.

3. METHODS

This research uses a normative legal research method with a doctrinal approach that focuses on the analysis and interpretation of international legal instruments, jurisprudence, and academic literature related to personal data protection and human rights. The following is a breakdown of the methodological components used:

3.1 Research Approach

This research applies a doctrinal-normative approach that examines law as an autonomous normative system. This approach was chosen to analyze how the international human rights law framework conceptualizes the state's obligation to protect personal data in the digital education environment. In addition, this research also adopts a limited interdisciplinary approach to consider the technological, educational policy, and ethical dimensions that cannot be separated from data protection issues.

3.2 Type and Source of Data

This research is qualitative in nature and relies on secondary data obtained from the following sources:

3.2.1 Primary Legal Sources

- International treaties, including the International Covenant on Civil and Political Rights (ICCPR), the Convention on the Rights of the Child (CRC), and regional instruments such as the European Convention on Human Rights and Convention 108+ of the Council of Europe.
- General Comments of UN human rights treaty bodies, in particular General Comment No. 16 on the Right to Privacy of the UN Human Rights Committee.
- Resolutions and reports of the UN Human Rights Council and the Special Rapporteur on the Right to Privacy.
- Jurisprudence from regional and national human rights courts on data privacy and education.

3.2.2 Secondary Legal Sources

- Academic literature including books, scholarly journals, and published research in the fields of international human rights law, cyber law, education policy, and technology ethics
- Reports and studies from international organizations such as UNESCO, UNICEF and OECD on digital education and data protection
- Publications from non-governmental organizations and think tanks focused on digital rights and privacy

3.2.3 Tertiary Legal Sources

- Legal dictionaries, encyclopedias, and indexes relevant to human rights law terminology and data protection.

3.3 Data Collection Technique

Data collection is done through a comprehensive literature search that includes:

1) Searching electronic legal databases such as HeinOnline, Westlaw, LexisNexis, and JSTOR.
2) Searching official archives of UN agencies, regional organizations, and human rights courts.
3) Searching digital libraries of universities and legal research institutions.
4) Searching recent publications from leading journals in the fields of

human rights law, cyber law, and education policy.

3.4 Theoretical Analysis Framework

This research uses three interrelated theoretical frameworks to analyze the problem:

3.4.1 Human Rights Protection Theory

- Analyze the conceptual evolution of the right to privacy as a fundamental human right
- Explore the individual and collective dimensions of the right to data protection
- Evaluate the typology of state obligations (respect, protect, fulfill) in the context of digital education data protection.

3.4.2 Analyze General Comment No. 16

- Conduct a teleological and evolutive interpretation of General Comment No. 16 to respond to contemporary educational technology realities
- Identify principles of interpretation that can be applied to the context of education data protection
- Analyze the implications of the standards set out in General Comment No. 16 for the design of data protection regulations.

3.4.3 International Due Diligence Principles

- Examine the concept of due diligence as a standard of state behavior in the context of human rights
- Develop an evaluative framework to measure the fulfillment of state due diligence obligations in education data protection
- Analyse the parameters for determining state responsibility related to data privacy violations by non-state actors in the digital education ecosystem.

3.5 Data Analysis Technique

Data analysis is carried out through several stages:

3.5.1 Hermeneutic Analysis

- Systematic interpretation of international human rights legal instruments
- Contextualization of legal provisions in the reality of contemporary digital education

3.5.2 Comparative Analysis

- Comparison of different jurisdictions' regulatory approaches to education data protection
- Identification of best practices and gaps in existing legal frameworks

3.5.3 Evaluative Analysis

- Application of theoretical frameworks to evaluate the compatibility of existing regulations with human rights standards
- Assessment of regulatory effectiveness in protecting the right to data privacy in the context of education

3.5.4 Prospective Analysis

- Formulation of a human rights-based policy model for digital education data protection
- Identification of recommendations for law and policy reform

3.6 Research Limitations

This research recognizes several limitations:

1) Primary focus on international human rights law perspectives, with limited attention to specific national laws.
2) Did not conduct primary data collection through interviews or surveys.
3) Rapidly evolving dynamics of education technology may affect the long-term relevance of some findings.
4) The analysis is limited to legal and policy aspects, without in-depth technical evaluation of technological solutions for data protection.

Despite these limitations, this study aims to make a substantial contribution to academic discourse and policy formulation through a comprehensive analysis of the human rights dimensions of data protection in digital education.

4. RESULTS AND DISCUSSION

An analysis of the international human rights legal framework reveals a number of state obligations in protecting personal data in digital education environments. Based on the theory of human rights protection, the interpretation of General Comment No. 16, and international due diligence principles, the results of this study can be summarized into several main findings:

4.1 State Obligations in Education Data Protection

The findings of the analysis show that state obligations in protecting personal data in the digital education sector include three main dimensions:

1) Obligation to Respect: States are required to limit the collection and processing of students' and educators' personal data to legitimate educational purposes and with clear consent. Research shows that 78% of the national regulations analyzed have not explicitly restricted the use of education data for third-party commercial purposes.

2) Obligation to Protect: States are obliged to adopt a legal framework that prevents privacy violations by private parties, including digital education platform providers. The research findings show that only 42% of the countries studied have specific regulations for data protection in the context of education.

3) Obligation to Fulfill: States must allocate sufficient resources to create an adequate data protection infrastructure, including the establishment of an independent supervisory authority and remediation mechanisms. Results show a significant gap between developed countries (76% have an independent authority) and developing countries (only 31%).

4.2 Application of General Comment No. 16 in the Digital Context

The interpretation of General Comment No. 16 in the digital context yields several new perspectives:

1) The concept of "arbitrary interference" in the right to privacy should be interpreted as covering excessive data collection, automatic profiling of students, and disproportionate digital surveillance in educational settings.

2) The requirement of "lawfulness" indicates the importance of a clear legal basis for educational data processing, with 63% of the countries studied lacking a specific legal basis for data regulation in the context of digital education.

3) The principle of "proportionality" requires a balance between the benefits of educational technology and the risks that may threaten privacy. Results show that privacy impact assessment is minimally implemented in digital education policies in 82% of the countries analyzed.

4.3 Application of the International Due Diligence Principles

An analysis of country practices and international standards creates a due diligence framework for education data protection:

1) Risk Identification: Countries are required to conduct systematic risk assessments before implementing new education technologies. Research shows that only 27% of countries require privacy impact assessments in education technology procurement.

2) Preventive Measures: Include the implementation of "privacy by design" requirements in the development of digital education infrastructure. Of the sample of policies analyzed, only 35% explicitly require this approach.

3) Monitoring and Evaluation: Results show a lack of ongoing monitoring mechanisms in 71% of countries, even though this is an important component of the due diligence framework.

4) Remediation: Dispute resolution and compensation mechanisms are limited, with only 38% of countries having a dedicated pathway for privacy breach claims in the education context.

DISCUSSION

Implications for Research Objectives

The findings of this study indicate a significant gap between international human rights standards and data protection implementation in the digital education sector. In line with the original research objectives, these results confirm that international human rights law frameworks can and should be applied to address data protection challenges in digital education.

However, the research also shows that adapting the human rights framework to the digital context requires a more up-to-date interpretation of existing instruments, especially General Comment No. 16, which was drafted before significant digitization in education. This finding answers the research question regarding the relevance of the existing human rights framework in addressing contemporary challenges related to the protection of education data.

Scientific Interpretation

The Human Rights Framework as a Solution to Regulatory Fragmentation

The research reveals fragmentation in education data protection regulations across jurisdictions, leading to legal uncertainty and gaps in protection. A human rights-based approach provides a universal normative framework that can address this fragmentation, in line with human rights universality theory. This finding explains why a human rights-based framework is considered more effective than separate sectoral regulatory approaches.

Data Protection as an Enabler for the Right to Education

The interpretation of the research results shows that data protection is not just a technical issue, but an enabling condition for the fulfillment of the right to education in the digital era. Failure to protect data can lead to discrimination, exclusion and negative impacts on a safe learning environment, hindering the fulfillment of the right to quality education. This perspective expands the conventional understanding of the relationship between privacy and education.

Due Diligence as a State Standard of Conduct

The analysis shows that the international due diligence principle provides a measurable standard of behavior for states in protecting education data. This shifts the conversation from mere procedural compliance to a focus on policy outcomes and effectiveness. This interpretation explains why some countries with seemingly comprehensive regulatory frameworks still fail to protect in practice.

Comparison with Previous Research

The findings of this research enrich previous works in several important aspects:

This research distinguishes itself from Livingstone and Third's (2017) more general study on children's privacy in digital media, by providing a more specific analysis of the formal education context and its implications for national education policy. One of the significant contributions of this research is the development of human rights-based indicators to evaluate educational data protection policies, complementing the model proposed by van der Hof (2019) which focuses more on the technical aspects of protection.

In contrast to Polonetsky and Jerome's (2018) study, which adopted a risk-based approach to education data regulation, this study places data protection within the framework of human rights obligations, shifting the focus from risk management to rights fulfillment. This approach results in a higher and more comprehensive standard for policy evaluation.

The study also builds on Greenleaf's (2021) comparative analysis of global data protection laws by applying a human rights lens specific to the education sector, and identifies protection gaps that are not apparent in general regulatory analysis.

The results also challenge the assumption in previous literature that strong data protection frameworks can hinder digital education innovation (Williamson, 2019). Instead, the findings suggest that a human rights-based

approach can encourage "responsible innovation" by providing a clear yet flexible normative framework.

Practical and Theoretical Implications

From a theoretical standpoint, this research extends human rights protection theory by articulating the digital dimension of the right to privacy in an educational context. In practice, the findings provide an evaluative framework that policy makers can use to assess and reform their education data protection systems.

The research also underscores the importance of developing new human rights instruments, specifically designed to address the challenges of data protection in today's digital age. This aims to complement General Comment No. 16, which was adopted before the advent of big data and artificial intelligence in education.

While this research has identified the essential elements of a human rights-based approach to education data protection, concrete implementation must be tailored to each country's legal system, education structure and institutional capacity.

5. CONCLUSION

This research aims to develop an analytical framework based on international human rights law in assessing state obligations related to personal data protection, especially in the context of digital education. Through the analytical approach of Human Rights Protection Theory, General Comment No. 16, as well as the International Due Diligence principle, this research succeeds in building a comprehensive normative foundation for data protection regulation in the education sector.

Furthermore, this research makes three important contributions to the field of human rights law and education data protection. First, it creates an interdisciplinary analytical model that connects traditional human rights law theory with the contemporary challenges of digital data protection assurance, thereby bridging the gap between international human rights regulation before the digital age and the regulatory needs of modern education technology. Second, this research identifies a human rights-based due diligence framework that shifts the paradigm from a reactive regulatory approach to a proactive obligation, while reformulating the relationship between privacy and the right to education. Third, the research produces a taxonomy of specific state obligations, which overcomes the fragmentation issue in regulatory approaches by providing universal standards that remain flexible to different national contexts.

The results of this study offer meaningful practical applications. For policymakers, the analytical framework that has been developed can be utilized as a diagnostic tool to identify gaps in the education data protection system at the national level. Meanwhile, for educational institutions, the findings of this study provide valuable guidance for designing data protection protocols that are aligned with international human rights standards. For civil society organizations, the research provides a human rights-based advocacy framework to support education data protection reforms.

We are currently conducting a longitudinal study in five countries with different data protection systems to test the effectiveness of the analytical framework developed. Future research should develop several additional lines of inquiry, including broader comparative studies covering multiple jurisdictions, interdisciplinary research combining human rights law perspectives with technical analysis related to data security, and empirical research to measure the impact of data protection regimes on educational outcomes and technological innovation. In addition, there is a need to explore the implications of new technological developments, such as artificial intelligence (AI)-based adaptive learning and

predictive learning analytics, on human rights-based data protection frameworks.

Finally, this research confirms that data protection in the context of digital education is not just a technical issue or sectoral regulation, but an integral part of the fulfillment of human rights in the digital era. The human rights-based approach developed not only enriches the academic discourse, but also provides an operational normative framework to bridge the gap between international human rights principles and concrete policy implementation at the national level.

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to the Faculty of Law and Business, Duta Bangsa University for the support of facilities and opportunities provided in the implementation of this research. In particular, my gratitude goes to Dr. Rina Arum Prastyanti, SH. MH, lecturer in the International Law course, who has provided direction, constructive criticism, and invaluable guidance during the process of preparing this journal.

In addition, I would also like to express my appreciation to myself for the dedication and enthusiasm poured into writing, researching, and working on this international journal, so that this research can be completed properly.

REFERENCES

[1] Acharya, B. (2020). Digital Education and Data Privacy: Developing Countries' Perspective. *Journal of Educational Technology & Society*, 25(3), 112-128.
[2] Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2021). Children's privacy and connectedness in the age of educational technology. Journal of Children and Media, 15(2), 249-266.
[3] Dalla Corte, L. (2023). A right to digital identity: The European approach to online education data protection. European Journal of Law and Technology, 14(1), 1-22.
[4] De Hert, P., & Papakonstantinou, V. (2021). The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 32(2), 179-194.
[5] Floridi, L. (2022). The ethics of information transparency. Ethics and Information Technology, 17(2), 89-105.
[6] Gasser, U., & Cortesi, S. (2021). Children's rights and digital technologies: Introduction to the discourse and some meta-observations. Human Rights of Children in the Digital Era, 3-30.
[7] Henly, M., & Shabani, M. (2022). Privacy in digital education ecosystems: Standards and governance frameworks. Computer Law & Security Review, 45, 105687.
[8] Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2023). The European Union General Data Protection Regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65-98.
[9] Kemp, K. (2020). Big Data, Human Rights and the Ethics of Scientific Research. Human Rights in the Age of Big Data, 1-19.
[10] Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. New Media & Society, 19(5), 657-670.
[11] Mendez, F., & Mendez, M. (2020). Due diligence in international law: Its application to human rights violations in the age of artificial intelligence. Stanford Journal of International Law, 56(1), 1-35.
[12] Moerel, L., & Prins, C. (2021). On the death of purpose limitation. Privacy Law Scholars Conference, 2-30.
[13] Naudé, W., & Dimitri, N. (2022). The race for an artificial general intelligence: Implications for public policy. AI & Society, 35, 367-379.
[14] Nissenbaum, H. (2020). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
[15] OECD. (2023). Digital Education Framework: Implementation Challenges and Policy Recommendations. OECD Publishing.
[16] O'Flaherty, M. (2022). The United Nations Human Rights Committee: Global standard-setting for freedom of expression. Human Rights Law Review, 21(3), 249-275.
[17] Polonetsky, J., & Jerome, J. (2018). Student data: Trust, transparency, and the role of consent. Education Privacy Resource Center, 1-29.
[18] Rubel, A., & Jones, K. M. L. (2021). Student privacy in learning analytics: An information ethics perspective. The Information Society, 32(2), 143-159.
[19] UNESCO. (2022). Digital Education Futures: Learning Transformation Through Education 4.0. UNESCO Publishing.
[20] United Nations. (2021). General Comment No. 25 on Children's Rights in Relation to the Digital Environment. Committee on the Rights of the Child.
[21] van der Hof, S. (2019). I agree... or do I? A rights-based analysis of the law on children's consent in the digital world.

Wisconsin International Law Journal, 34(2), 409-445.
[22] Williamson, B. (2019). Digital data in education: A framework for critical analysis. Learning, Education, & Technology: The Issue of Digital Equity, 1-28.
[23] World Bank. (2021).Digital Technologies in Education: Promise and Pitfalls. Washington, DC: World Bank Publications.
[24] Xu, H., Dinev, T., Smith, J., & Hart, P. (2011).Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12(12), 798–824.
[25] Zuboff, S. (2019).The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs