
**DIGITAL EDUCATION AND DATA PRIVACY UNDER NEP 2020: A
LEGAL ANALYSIS OF THE DPDP ACT, 2023 TOWARDS VIKSIT
BHARAT@2047**

***Lokanath Patra**

Research Scholar (Law), Berhampur University, Odisha.

Article Received: 05 June 2026

*Corresponding Author: Lokanath Patra

Article Revised: 25 June 2026

Research Scholar (Law), Berhampur University, Odisha.

Published on: 15 July 2026

DOI: <https://doi-doi.org/101555/ijrpa.4844>

ABSTRACT

The National Education Policy (NEP) 2020 promises a dramatic transition to digital education, fostering accessibility, diversity, and technological integration within India's educational framework. The growing reliance on online platforms, virtual classrooms, and EdTech applications has led to a substantial increase in the collection and processing of students' personal data, thereby raising significant concerns about privacy and data protection.

The Digital Personal Data Protection Act, 2023 (DPDP Act) establishes an essential legal framework for regulating data processing operations and protecting individual privacy. Educational institutions and EdTech platforms, acting as data fiduciaries, are now accountable for ensuring authorized processing, obtaining valid consent, and upholding data security, especially regarding minors' data.

This paper employs a doctrinal research method to rigorously analyze the convergence between the NEP 2020 and the DPDP Act, 2023. It assesses whether the current legal framework adequately addresses developing concerns, including informed consent, data breaches, algorithmic profiling, and the commercialization of educational data. The paper contextualizes these challenges within the overarching constitutional framework of the right to privacy as acknowledged by the Supreme Court of India.

The study contends that whereas NEP 2020 robustly promotes digital transformation, it lacks a robust data governance framework, thereby requiring effective enforcement of the DPDP Act. It concludes with ideas for strengthening regulatory compliance, enhancing institutional

accountability, and ensuring ethical data practices. These approaches are crucial for fostering trust in digital education and realizing the vision of Viksit Bharat@2047.

KEYWORDS: NEP 2020, Digital Education, Data Privacy, DPDP Act, 2023, EdTech Regulation, Right to Privacy, Educational Governance, Viksit Bharat@2047.

INTRODUCTION

The national vision of Viksit Bharat@2047 relies on reforming the digital education system. The National Education Policy (NEP) 2020 emphasizes digital infrastructure, technology integration, and learner-centric pedagogy to create a globally competitive knowledge economy (Ministry of Education, 2020). Digital education has gone from a complement to a major part of mainstream learning post-pandemic, accelerating this shift.

One of the largest education ecosystems in the world, India has 24.8 crore (248 million) students in 14.72 lakh institutions and roughly 98 lakh teachers (Economic Survey 2024–25). From 22.3% in 2019–20 to 53.9% in 2023–24, schools with internet connections, and from 38.5% to 57.2% with computers, show rapid growth in digital infrastructure. These advancements demonstrate the widespread adoption of digital technologies in education.

In parallel, the Indian EdTech business has grown exponentially, driving educational reform. The USD 7.5 billion sector is expected to grow to over USD 30 billion by 2030–31, making India the second-largest e-learning market. Recent trends show that 35% of Indian school EdTech users are already using generative AI tools in learning, showing the growing relevance of advanced technology in education.

This rapid digitalization has also led to unprecedented increases in the collection, processing, and monetization of personal data, especially of minors. Educational platforms capture personal data, academic records, behavioral analytics, and location data. Informational privacy, surveillance, and data exploitation are important challenges.

The severity of cybersecurity risks emphasizes the need to address them. Recent studies show that Indian educational institutions are among the most attacked globally, with about 7,000 to 8,000 cyberattacks each week, above global averages. Worse, a 2025 study found that Indian educational institutions experienced over 2 lakh intrusions and nearly 4 lakh data breaches in 9 months, highlighting cybersecurity flaws. Overall, cyber incidents in India rose from 1.03

million in 2022 to over 2.27 million in 2024, underscoring the threats to the digital ecosystem.

Justice K.S. Puttaswamy v. Union of India (2017) established the Right to Privacy as a fundamental right under Article 21. These developments must be analyzed within that framework. Informational privacy is essential to human dignity and autonomy, and any invasion must be legal, necessary, and proportional, the Court said. This principle is especially important in digital education, because students—especially minors—are increasingly monitored and profiled.

To address these issues, the Indian government enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), which regulates the processing of personal data. The Act establishes data fiduciaries, data principals, consent-based processing, purpose limitation, accountability mechanisms, and kid data protections, including monitoring and targeted advertising (MeitY, 2023).

Despite legislative progress, the policy-driven expansion of digital education under NEP 2020 and regulatory safeguards under the DPDP Act, 2023, remain at odds. NEP 2020 emphasizes technological integration but ignores data governance, cybersecurity, and institutional accountability. Digital innovation advances faster than legal and ethical safeguards in this regulatory vacuum.

Thus, digital education and data privacy create complex legal and regulatory issues. This paper critically assesses the DPDP Act, 2023, and its data regulation within the NEP 2020 through doctrinal research. While India is moving toward digitally empowered education, the lack of a comprehensive, sector-specific data governance policy threatens fundamental rights and public trust.

Thus, strong data protection is not just a legal requirement but also a prerequisite for sustainable, inclusive, and rights-based digital education, which is important to Viksit Bharat@2047.

MATERIALS AND METHODS

This study adopts a doctrinal legal research methodology. It relies on analysis of primary sources, including the Constitution of India, the Digital Personal Data Protection Act, 2023, judicial decisions, and the National Education Policy 2020, as well as secondary sources such

as government reports, journal articles, policy documents, and international literature. A qualitative, analytical, and comparative approach is employed to evaluate the legal framework governing data privacy in digital education and to identify regulatory gaps and policy implications.

RESULTS AND DISCUSSION

1.1 Digital Education Ecosystem: Scale, Penetration, and Technological Expansion

Digital education in India has become a complex ecosystem integrating ICT, AI, and data-driven learning systems. This shift is unprecedented. India had approximately 886 million internet users in 2024, with nearly 55% in rural areas, expanding digital education beyond urban centers. As schools with internet access increased from 22.3% in 2019–20 to over 53.9% in 2023–24, and forecasts anticipate over 63% connectivity in 2024–25, institutional digital preparedness increased.

EdTech drives this ecosystem. Smartphone adoption, low-cost internet, and NEP 2020 policy measures are expected to raise India's EdTech sector from USD 7.5 billion to USD 29–30 billion by 2030. The global EdTech business was worth USD 142.37 billion in 2023 and is projected to grow by over 13% through 2030, reflecting a systematic shift toward technology-mediated education.

Digital channels now account for over 62% of student enrolments in India, normalizing online platforms in educational decision-making and delivery. Some studies show a 25% increase in student engagement and demonstrable learning results with AI-based tools and adaptive learning systems.

Educational records and student identities have been digitized due to technological advancements. NEP-driven efforts like the Academic Bank of Credits (ABC) are digitizing millions of student records, with one state-level project reporting over 14 million student data entries across institutions. This highlights the growing importance of data in educational governance and administration.

1.2 Datafication of Education: Nature, Volume, and Economic Value of Data

The “datafication” of education involves using digital platforms to quantify learning processes. Modern digital education systems treat students as data subjects, collecting personal and behavioral data. Educational platforms collect many types of data: Personal data

(name, age, location, contact info), Academic data (grades, performance measures, attendance), Data on engagement, response times, and learning preferences, and Device and metadata (IP addresses, browsing history, geolocation). This data is growing exponentially due to user interaction and platform dependencies. India's online education market reached USD 3.6 billion in 2025 and is expected to grow at a CAGR of over 23% through 2034, driven by a surge in data collection and processing.

Student data is valuable in the digital market. EdTech uses data analytics for Personalized learning suggestions, conducts targeted advertising, and develops and optimizes products. Studies show that personalized algorithmic recommendations can boost platform usage by 60%, linking data consumption to commercial value. This fits into “surveillance capitalism,” where user data is sold for profit. However, these techniques pose challenges regarding data ownership, permissions, and ethical use, especially for minors.

1.3 Data Governance in Digital Education: Regulatory and Institutional Dimensions

Data governance in digital education governs data collection, storage, processing, and distribution through rules, regulations, and institutions. It includes principles like Autonomy and consent, Purpose limitation, Minimizing data, Safeguards for security, and Transparency and accountability. Governance frameworks have lagged behind the rapid expansion of digital education. Studies show that many institutions lack digital competence and regulatory readiness, causing disparities, learning gaps, and governance inefficiencies.

Cybersecurity risks worsen data governance issues. Weak infrastructure and compliance processes make schools more susceptible. India has millions of cyber incidents per year, indicating systemic risks in managing critical educational data. Governance issues arise when AI and learning analytics are combined. Data-driven technologies fuel innovation but raise difficult privacy, ethics, and accountability issues, according to OECD analysis. The digital divide also threatens the equity of digital education. Digital literacy and access are inconsistent in rural and underprivileged populations, despite infrastructure improvements. This presents a challenge in promoting digital education while maintaining inclusive, rights-based data governance.

1.4 Emerging Risks: Privacy, Surveillance, and Algorithmic Governance

Several legal and ethical risks have arisen from digital schooling and data stewardship.

Data breaches and privacy risks: Data breaches are more likely with large-scale student data storage. Educational platform breaches have exposed millions of student records, including sensitive personal data, showing security weaknesses.

Algorithmic Monitoring and Profiling: Continuous student behavior monitoring using AI-based learning systems results in Predictive profiling, Score by behavior, and Automated decision-making. Loss of autonomy, prejudice, and bias are problems, especially in the absence of openness.

Commercial data exploitation: Targeted advertising and third-party exchange of student data raise ethical concerns. Over 62% of enrolments are driven online, and platforms rely on data analytics for revenue.

Governance Deficit and Regulatory Lag: The education sector has limited application of legal frameworks such as the DPDP Act, 2023. The lack of sector-specific norms leads to confusion in compliance and enforcement.

1.5 Towards a Data-Driven but Rights-Oriented Educational Framework

Digital education and data governance show a conflict between technology and rights. Digital technologies improve the accessibility, efficiency, and customization of education. However, they raise complex privacy, surveillance, and ethical issues related to data. The Indian digital education ecosystem features Rapid technical growth, exponential data generation, growing economic importance of data, and Insufficient governance structures.

A rights-oriented data governance framework that balances technological innovation with constitutional privacy, dignity, and autonomy is needed to reconcile these dynamics. The framework must include Legal safeguards (DPDP Act, 2023), Policy orientation (NEP 2020), Institutional accountability, and Ethical AI practices. Only an integrated approach can ensure that India's digital education ecosystem efficiently supports Viksit Bharat@2047 while protecting basic rights.

2. Constitutional Foundations of Data Privacy in India

2.1 Indian Privacy Jurisprudence Evolution

Indian courts have interpreted the Constitution to protect privacy in the absence of specific language. Although the Indian Constitution did not specifically guarantee privacy, judicial judgments bolstered Article 21, which guarantees life and personal liberty.

M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962) limited privacy as a right. Gobind v. State of Madhya Pradesh (1975) and R. Rajagopal v. State of Tamil Nadu (1994) established privacy as a constitutional right.

In Justice K.S. Puttaswamy v. Union of India, a nine-judge bench of the Supreme Court unanimously upheld the Right to Privacy under Article 21 and Part III of the Constitution, a major jurisprudential shift.

2.2 Puttaswamy Judgment: Informational Privacy Doctrinal Framework

The Puttaswamy judgment constitutionally redefined digital governance and data protection. The Court said privacy was a multidimensional right, encompassing Body privacy, Decision-making autonomy, and privacy of information.

Informational privacy is the individual's right to control the dissemination and use of personal data related to digital schooling. Personal data extends dignity and personality in the digital age, the Court said. The judgment created a four-step proportionality doctrine for privacy violations:

1. Legality – existence of a valid law
2. Legitimate State Aim – necessity of the objective
3. Proportionality – rational nexus between means and objective
4. Procedural Safeguards – protection against abuse

Digital education relies on this structure since state-run platforms like DIKSHA and private EdTech companies manage large volumes of data. An activity must meet these constitutional conditions.

2.3 Digital Education and Information Privacy

Digital education systems capture student identities, academic performance, behavioral analytics, and biometrics. Important informational privacy issues arise. In Puttaswamy, the Supreme Court warned against a "surveillance state" that may undermine personal sovereignty through unfettered data collection. Continuous AI-driven school monitoring may lead to behavior tracking, Student profiles, and automated decision-making. Such approaches may violate pupils' informational self-determination, especially minors.

Empirical data show its extent. Over 248 million schoolchildren and 35% of EdTech users employing AI tools generate unprecedented student data. Education data is crucial in the digital economy.

2.4 Expanding Constitutional Values: Privacy, Dignity, Autonomy

Privacy is tied to the dignity, autonomy, and liberty protected by Article 21. In Puttaswamy, the Supreme Court underlined that privacy is essential for other fundamental rights:

- Freedom of expression (Article 19(1)(a))
- Free association (Article 19(1)(c))
- Article 21A: Education rights

Privacy violations may chill education, including intellectual freedom, Academic participation, and the psychological well-being of students. Self-censorship and stress from algorithmic monitoring of student performance may undermine the holistic education aims of NEP 2020. Informational asymmetry—where organizations control personal data disproportionately can lead to exploitation and coercion, the Court said. In EdTech, users often sign complex privacy terms without understanding.

2.5 Child Privacy and Constitutional Rights

Education data privacy requires protecting children's data. Through judicial interpretation, the Constitution recognizes improved child protection. The Supreme Court in Puttaswamy noted vulnerable populations need stronger data protection. This follows Directive Principles such as Article 21, Articles 39(e) and (f), which protect children against exploitation, and Article 45, which concerns Early Childhood Education and Care.

Digital learning exposes youngsters to targeted advertising, Behavior profiling, and data monetization methods. An estimated 2 lakh cyberattacks and 4 lakh data breaches have exposed massive amounts of student data in Indian educational institutions. These examples demonstrate the need for constitutional safeguards in child-related digital contexts.

2.6 Privacy and State/Non-State Actors

The Puttaswamy Court recognized that commercial enterprises have privacy obligations too. This matters in the digital education ecosystem because EdTech platforms save data, Private entities own massive student data, and Common international data flows. The Court highlighted the need for strong data protection legislation to govern private actors and

prevent data exploitation. The 2023 Digital Personal Data Protection Act was founded on this constitutional requirement. The constitution requires public and private EdTech firms to maintain legal data processing, Secure data, and honor individual autonomy.

2.7 Constitutional Limits and Regulation

The recognition of privacy as a fundamental right is a tremendous achievement, but its enforcement requires legal and institutional processes. The Supreme Court in Puttaswamy recognized the necessity of a comprehensive data protection law. However, issues such as the lack of sector-specific education rules, poor understanding of privacy rights among stakeholders, and Weak enforcement methods persist. Digitization has outpaced regulatory preparation in education, highlighting the mismatch between constitutional aspirations and practice.

2.8 Digital Education Constitutionalism

The Indian Constitution protects data privacy with dignity, autonomy, and liberty. Informational privacy is essential, making the digital education ecosystem regulation solid. The practical application of these principles requires constitutional policy alignment (NEP 2020), the successful implementation of the DPDP Act, 2023, protections, and Institutional awareness and responsibility.

Viksit Bharat@2047 must ensure constitutional rights are respected during digital transformation. Instead, create an innovative, privacy-focused, rights-centric digital education environment.

3. India's Data Protection Framework: Legal Architecture and Educational Implications

India's evolution toward a comprehensive data protection regime has been gradual and shaped by technological advancements and judicial rulings. Initially, data protection was managed under the fragmented framework of the Information Technology Act, 2000, which imposed minimal obligations and lacked enforceability. The recognition of privacy as a constitutional right in the landmark case of Justice K.S. Puttaswamy v. Union of India prompted the call for robust data protection legislation, leading to the establishment of the Justice B.N. Srikrishna Committee in 2017. This culminated in the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), which aims to balance individual privacy rights with the need for digital innovation.

The DPDP Act introduces a structured framework for personal data processing and aligns closely with global data protection standards, such as the GDPR, while adapting to the Indian context. Key principles of the Act include the need to obtain explicit consent for data processing, limitations on data collection to specific and lawful purposes, and the requirement to maintain data accuracy and to impose retention limits. It categorizes educational institutions and EdTech platforms as data fiduciaries responsible for compliance, with additional obligations for significant data fiduciaries, including data audits.

Particularly notable is the Act's emphasis on protecting children's personal data through provisions such as mandatory parental consent and prohibitions on tracking and targeted advertising aimed at minors. However, implementation challenges persist, particularly concerning reliance on default consent mechanisms without adequate age verification.

The DPDP Act establishes the Data Protection Board of India (DPBI) as the primary authority for monitoring compliance and adjudicating disputes, with significant penalties for violations. Nonetheless, concerns remain about the Board's independence and capacity, as well as the absence of targeted guidelines for educational data processing.

Despite the DPDP Act, challenges persist in the education sector. The lack of sector-specific regulation creates compliance ambiguity, and many institutions exhibit limited awareness and capacity in data protection. Moreover, educational institutions face rising cybersecurity threats, with data breaches becoming increasingly common. Concerns regarding cross-border data transfers further complicate the regulatory landscape.

Comparative perspectives reveal that while India's framework is developing, it still falls short of global best practices. The GDPR emphasizes strong rights for data subjects and imposes strict penalties, while U.S. regulations such as COPPA and FERPA set clear obligations for educational institutions. India's general framework may not adequately address the complexities of the educational sector.

The relationship between policy and law, particularly given the NEP 2020's advocacy of digital education, exposes gaps in data governance and compliance standards. This disconnect highlights the need for a cohesive strategy that harmonizes regulatory safeguards with educational innovation.

In conclusion, India's data protection framework, led by the DPDP Act, marks significant progress in privacy protection. Still, its effectiveness in the education sector requires the development of sector-specific guidelines, enhanced institutional capacity, increased awareness among stakeholders, and robust enforcement mechanisms. Achieving a balanced regulatory ecosystem is crucial for ensuring that India's digital education advancements are sustainable and respectful of constitutional principles of privacy.

4. Key Privacy Challenges in Digital Education: Empirical Trends and Case Studies

4.1 Large-Scale Data Collection and Datafication of Students

Since education has gone digital, student data collection has skyrocketed, often without adequate safeguards. Students generate data continuously as digital education systems collect fundamental demographic, behavioral, biometric, and interaction data. The “datafication of education” raises important questions about proportionality and necessity.

Evidence suggests India's education sector is increasingly data-intensive. Login credentials, learning data, and performance tracking are collected when millions of students utilize EdTech platforms daily. Studies show that many platforms collect more data than necessary for educational purposes, violating the principle of data minimization. EdTech data leaks exposed student records, email addresses, and payment details, raising concerns about data management. Data accumulation heightens concerns about abuse and builds long-term digital profiles that may affect students' academic and professional opportunities.

4.2 Cybersecurity Threats and Data Breaches in the Education Sector

Cyberattacks on educational institutions are a big issue in digital education. Education is one of the most vulnerable digital domains due to insufficient infrastructure, limited cybersecurity expertise, and the high value of student data. Over 2 lakh cyberattacks and 4 lakh data breaches occurred at Indian educational institutions in 2025, indicating a systemic catastrophe. The sector has 8,000–8,487 weekly cyberattacks, double the global average. Examples include phishing, ransomware, credential theft, and AI-driven cyberattacks. Indian digital ecosystems are vulnerable to cybersecurity events, which climbed from 10.29 lakh in 2022 to 22.68 lakh in 2024. Cybercriminals target schools lacking IT infrastructure.

Case Study: Data Breaches in Educational Institutions (India, 2025)

The CyberPeace Foundation revealed that large cyberattacks and data breaches at Indian educational institutions exposed student names, academic records, and financial information.

Poor cybersecurity frameworks, encryption, and compliance standards were major factors, the survey said. This scenario emphasizes institutional data protection and cybersecurity checks.

4.3 Lack of Informed Consent and Children's Data Vulnerability

Digital education is plagued with uninformed consent, especially for minors. Most EdTech platforms have confusing, bundled privacy policies that kids and parents don't understand. The 2023 DPDP Act requires verified parental consent to process children's data, although in practice, poor age-verification methods, Implied consent, and Users must accept educational service agreements are common. Forced consent weakens data principle autonomy.

Case Study: EdTech Privacy Practices in India

EdTech platforms, reports say, share data with advertisers, track behavior with tools, have limited transparency into data use, and target advertising and profiling of youngsters, creating ethical and constitutional issues. Experts say India's regulatory system, without sector-specific data norms for children's education, raises vulnerabilities.

4.4 Algorithmic Surveillance, AI Profiling, and Behavioral Tracking

AI and learning analytics have generated algorithmic surveillance, a privacy threat. Digital platforms monitor student behavior, time spent on tasks, Learning styles, Engagement levels, and Complex system emotions. These technologies promote tailored learning but also enable predictive profiling and automated decision-making, which may lead to prejudice, discrimination, and a loss of autonomy.

Case Study: AI-Based Facial Recognition in Schools (Karnataka)

Schools proposed AI-driven facial recognition systems for attendance monitoring, raising privacy concerns. Such systems could, experts warned, cause data sharing without consent, Identity theft and misuse, and the monitoring of kids. The concept was attacked for turning schools into surveillance zones and for compromising privacy. This case shows how technological efficiency and fundamental rights collide, especially in education.

4.5 Commercialization and Monetization of Student Data

Commercialization of education has made student data valuable. The EdTech uses data for targeted advertising, product development, and revenue-generating analytics. In “surveillance capitalism,” user data is sold without consent.

Research shows that data-driven platforms boost user engagement and profitability, leading to excessive data collection. However, these practices raise severe concerns about Ethics in data use, the exploitation of minors, and a Lack of transparency.

Case Study: EdTech Data Monetization Practices

EdTech platform studies showed that third parties got student data, targeted marketing with behavioral analytics, and Privacy protections were inadequate. These findings underscore the importance of ethical data stewardship and strict regulation.

4.6 Institutional Weaknesses and Governance Deficit

Educational institutions' unwillingness to adopt data protection regulations is another concern. Many schools and universities lack Dedicated data protection officers, Cybersecurity infrastructure, and data governance standards. Although knowledgeable, over 53% of teachers had experienced cybercrime, suggesting that preventive and reactive measures were inadequate. The lack of sector-specific criteria in the DPDP Act makes compliance unclear and inconsistent across institutions.

4.7 Structural Risks: Digital Divide and Inequality

Access to digital education deepens structural inequality. Rural and poor pupils face Limited secure access to digital devices, a lack of digital literacy, and rising cyberfraud risks. Rapid digital platform expansion without safeguards creates two risks: 1. Exclusion from digital education, and 2. Digital system abuse. Digital education privacy issues are legal, socio-economic, and developmental.

4.8 Multi-Dimensional Nature of Privacy Challenges

Multi-layered and systematic digital education privacy issues include: Tech hazards (AI surveillance, data breaches), Lack of sector-specific regulations, Institutional weaknesses, limited compliance, Data monetization—economic abuse, and Digital gap (social inequality) These factors create a high-risk data environment, especially for children who use digital education platforms the most.

These difficulties require a holistic approach that includes the constitution, which protects privacy, dignity, and individuality; legal frameworks (2023 DPDP Act); policy initiatives (NEP 2020); and institutional responsibility and awareness. India requires a secure, ethical, and aligned digital education plan aligned with Viksit Bharat@2047.

CONCLUSION

Digitalization has fundamentally changed India's education system. Viksit Bharat@2047 says digital education can democratize access, increase learning, and create a knowledge-based economy. National Education Policy (NEP) 2020 encourages digital infrastructure, innovation, and technological integration, supporting this shift. However, fast expansion has complicated data protection and control.

The DPDP Act was used to examine digital education and data protection critically. India has made progress in data privacy legislation, but it is insufficient to handle education's unique challenges. The lack of sector-specific legislation, institutional capacity, and consent-based procedures leads to reactive, fragmented, and unaligned policies. Policy aims and legal safeguards differ systemically, according to this analysis. Data governance, privacy, and ethical use of technology are lacking in NEP 2020's data-driven, technology-enabled education environment. Instead, the DPDP Act, 2023 provides a generic data protection framework without contextual specificity for educational data regulation, such as minors, algorithmic decision-making, and long-term data retention.

The empirical findings of this study highlight the need to close these gaps. Cyberattacks, data breaches, and data exploitation leave schools and children vulnerable in the digital market. In Justice K.S. Puttaswamy v. Union of India, the Supreme Court highlighted that large-scale student data collection and processing—often without informed consent—raises concerns about privacy, autonomy, and dignity. AI and learning analytics introduce algorithmic monitoring, profiling, and bias that the law does not regulate. Using educational data for profit conflicts with constitutional rights.

This paper proposes rights-based data governance for digitally enabled education, grounded in these findings. This framework should anticipate and regulate new issues. Technology innovation must not infringe constitutional rights, including privacy, dignity, autonomy, and proportionality. Many criteria arise for this. First, education sector-specific data protection policies should address the protection of student data and the dangers to minors. Data protection, cybersecurity, and compliance must improve institutional capacities. Third, the regulatory framework must include data audits and impact evaluations, not only consent, but also to ensure accountability and risk management. Fourth, digital education governance must include ethical AI principles that promote openness, justice, and human oversight.

Digital literacy and awareness are essential for kids, parents, educators, and administrators. Even robust laws might collapse without informed involvement. The digital divide must be addressed to guarantee that digital education serves everyone and does not aggravate inequality. India's digital education future depends on policy, law, and the integration of technology. The Viksit Bharat@2047 vision demands technology and protection of constitutional and human rights. Digital education must become a trust-based ecosystem with balanced innovation, accountability, access, and security.

In conclusion, India is leading a digital education revolution, but its success depends on how successfully it integrates privacy, ethics, and governance. A sustainable, inclusive, and legally coherent digital future requires rights-centric data governance.

ACKNOWLEDGEMENTS

The author expresses sincere gratitude to Berhampur University and all scholars whose work has contributed to this study. No external funding was received for this research.

REFERENCES

1. All India Survey on Higher Education (AISHE). (2022). *All India Survey on Higher Education 2020–21*. Ministry of Education, Government of India.
2. Economic Survey. (2024–25). *Education sector statistics*. Government of India.
3. Ministry of Education. (2020). *National education policy 2020*. Government of India.
4. Ministry of Education. (2024). *UDISE+ report on school education in India 2023–24*. Government of India.
5. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act, 2023*. Government of India.
6. Press Information Bureau. (2024). *Digital infrastructure in school education*. Government of India. <https://www.pib.gov.in>
7. CERT-In. (2023). *Annual report on cybersecurity incidents*. Indian Computer Emergency Response Team, Government of India.
8. CERT-In. (2024). *Cyber security incident statistics and trends*. Government of India.
9. CyberPeace Foundation. (2025). *Cyber threats in the Indian education sector*. CyberPeace Foundation.
10. Internet Freedom Foundation. (2022). *Privacy and data protection concerns in EdTech sector*. Internet Freedom Foundation.

11. IBEF. (2024). *Education and EdTech industry in India*. India Brand Equity Foundation.
<https://www.ibef.org>
12. KPMG. (2023). *India EdTech market outlook*. KPMG India.
13. IMARC Group. (2025). *India online education market report*. IMARC Services Pvt. Ltd.
14. OECD. (2025). *Digital technology and data governance in education*. Organisation for Economic Co-operation and Development.
15. UNESCO. (2022). *Education in a post-COVID world: Nine ideas for public action*. UNESCO.
16. World Bank. (2022). *World development report 2021: Data for better lives*. World Bank.
17. Justice B.N. Srikrishna Committee. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Government of India.
18. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
19. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
20. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
21. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
22. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
23. Information Technology Act, 2000 (India).
24. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
25. Digital Personal Data Protection Act, 2023 (India).