Vol. 2, Issue 1, August 2025 Subject-Law ISSN 3049-3099 (Print)

Peer Reviewed

VIPS JOURNAL OF LAW & DEVELOPMENT

VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES-TC (VIPS-TC)
Affiliated to GGSIP University, Delhi & Approved by Bar Council of India & AICTE
Grade 'A++' Accredited Institution by NAAC &
Recognized by UGC under Section 2 (f) & NBA Accredited for MCA Programme
ISO 9001:2015 Certified Institution

About Vivekananda Institute of Professional Studies – TC (VIPS-TC)

Vivekananda Institute of Professional Studies - TC (VIPS-TC) was established in the year 2000. Even as a sapling, its roots were firm, for they were energized by Swamiji's teachings. Today, VIPS – TC has progressed and is nestling sixteen courses under seven different Schools. It continues to stand with determination, moral sight and strength of mind to create capable and ethical human beings with infinite power, infinite knowledge and indomitable positive energy. Under the aegis of VIPS – TC, Vivekananda School of Law and Legal Studies (VSLLS) is committed to realizing the words of Swami Vivekananda: "Man Making, Character Building and Nation Building" and is well known for its robust efforts in legal education. Research is integral to academics as it forms the foundation for knowledge creation and intellectual growth. It enables students, scholars, and professionals to explore new concepts, test theories, and contribute to the existing body of knowledge in their respective fields. VSLLS works towards development oriented research in the Legal domain.

About the VIPS Journal of Law & Development

VIPS Journal of Law & Development is an annual double blinded peer reviewed journal accepting submissions in English language. The inception year of the Journal is 2024 and it is further envisioned to promote global development of Law as it provides a platform for scholarly research dedicated to exploring the intersection of legal frameworks and socio-legal development with an inter disciplinary approach. The Journal follows transparent review policy, ensuring that all submissions undergo rigorous scrutiny through a double- blind peer review process by subject experts, maintaining academic integrity. As a policy of the Journal the contributing authors are communicated the comments and suggestions from the reviewers and are also regularly updated about the status of their submission. The mode of citation for the journal is VIPS VSLLS VOL 2 VJLD (2025).

TABLE OF CONTENTS

Title of the Paper / Author	Page No.
An Appraisal of Arbitration Laws in India *Dr. Chandrakanthi L*	**1**
From Crisis To Circularity: A Legal Perspective on E-Waste Management in India *Dr. Gunjan Ahuja & Dr. Ankita Kumar Gupta*	**23**
Green Economy: Catalysing Sustainable Development in India *Dr. Sadaf Moosa*	**37**
Judicial Discretion and Sentencing: Balancing Justice, Proportionality, and Reform in Indian Criminal Law *Shashank Raghav*	**56**
Reforming Juvenile Justice In India: The Role of Victim-Offender Mediation in Diversion and Rehabilitation *Chinki Verma*	**81**
Advancing Circular Economy through Extended Producer Responsibility in India *Vagisha Nandini*	**100**
Mental Health Laws in India: Unveiling the Legal Landscape *Srishti*	**124**
Reforming the Indian Matrimonial Law: The Case for Recognizing Pre-Nuptial Agreements in India's Pluralistic Society *Rupal Gupta*	**142**
Judiciary's Role In Tackling Non-Performing Assets in The Indian Banking Sector *Dikshant Gupta*	**156**

Beyond Consent: The New Frontier of Children's Privacy Rights in India's DPDP Act **176**
Ananya Tiwari

Navigating gig work in India's New Labour Codes: Legal Challenges, Global Insights, and the Path to Social Security **192**
Pallavi Kumari

Digital Dystopias: Legal Quandaries of Innovation, Accountability, And Rights in the Metaverse **210**
Shambhawi Tiwari & Akanksha Aditi

Patent Illegality in Arbitration: Aligning Indian Jurisprudence with Global Standards **223**
Disha Bhatia

Weaponized Code: The Use of Automated Systems to Sort, Control and Exclude Refugees **234**
Manshwi Anand

Submission Guidelines **256**

BEYOND CONSENT: THE NEW FRONTIER OF CHILDREN'S PRIVACY RIGHTS IN INDIA'S DPDP ACT

Ananya Tiwari*

VIPS Journal of Law & Development
Subject - Law
August 2025, Vol. 2, Issue 1, 176-191
ISSN 3049-3099 (Print)
©Vivekananda Institute of Professional Studies-TC
(VIPS-TC)
https://vslls.vips.edu/vslr/

ABSTRACT

The research article aims to examine the Digital Personal Data Protection Act (DPDP) 2023 and its companion Rules of 2025 as this is India's landmark legislative response to protecting children's privacy rights in the digital age. The research article aims to analyze the comprehensive framework established for safeguarding minors' personal data, evaluate compliance requirements for data fiduciaries, and assess the Act's effectiveness in addressing emerging challenges posed by artificial intelligence and educational technology platforms. The research article examines India's DPDP framework alongside established international regulations including the European Union's General Data Protection Regulation (GDPR) and the United States' Children's Online Privacy Protection Act (COPPA). The research article reveals that India's DPDP Act establishes one of the most comprehensive global frameworks for children's data protection by setting the age threshold at 18 years, higher than both GDPR (16/13 years) and COPPA (13 years). The Act mandates verifiable parental consent through innovative mechanisms, including Digital Locker integration and government-authorized verification systems. However, the research article also identifies critical gaps in addressing AI-powered data processing, particularly in educational technology environments where traditional consent mechanisms prove inadequate. The "datafication of childhood" presents unique challenges as AI systems enable sophisticated behavioral profiling and automated decision-making that extends far beyond initial data collection purposes. The findings reveal that while the DPDP Act

* 3rd Year Law Student, B.A. LL.B. (Hons.), Dr. BR Ambedkar National Law University, Sonipat.

establishes robust foundational protections, the rapid advancement of AI technologies, particularly in EdTech platforms, necessitates domain-specific regulatory guidance to address emerging risks effectively. As India's digital economy continues to expand and children's online presence grows, this research article provides essential insights for policymakers, legal practitioners, and technology companies seeking to ensure compliance while fostering innovation in child-safe digital environments.

Keywords: *Digital Data Protection Act, Privacy Rights, Child Rights, Datafication, Parental Consent*

1. INTRODUCTION

The Digital Personal Data Protection Act[1] (herein after referred to as "DPDP") of 2023 and its companion Rules of 2025 represent a watershed moment in India's approach to protecting citizens' privacy rights in the digital age, with particularly significant implications for children. When we look at the current scenario, the concept of privacy is something that originated in the last 5-10 years. Still, it's pretty essential now since we live in times where the online lives of children start at birth with their every step being documented and put online. The government has taken a landmark step towards the personal data protection of all with the DPDP Act that was released in 2023 and its subsequent Rules[2] that were released in 2025. This legislative framework represents a comprehensive attempt to safeguard personal information, with special provisions that recognize children as uniquely vulnerable digital citizens since they don't know or understand the meaning of consent or what they are dealing with in the online realm. DPDP act and rules present a structured legal framework since privacy is a fundamental right of the citizen guaranteed under the Constitution of India, but how society values and safeguards the privacy of its youngest citizens is quite essential in nature.[3]

The DPDP Act emerges at a critical juncture. Today's children[4] are the first generation

1 Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

2 Ministry of Electronics and Information Technology, https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jan/doc202515481101.pdf, (last visited Apr. 8, 2025)

3 Justice KS Puttaswamy (Retd.) and Anr. v. Union of India, [2017] 10 S.C.R 569.

4 UNICEF for every child, https://www.unicef.org/childrightsandbusiness/media/226/file/Brief-Children-and-Online-Privacy.pdf , (last visited Apr.8, 2025.)

to have their entire lives from ultrasound images to school achievements to teenage social media posts documented online, often before they can meaningfully consent or manage which aspects to show on the internet and from where to refrain. This "datafication of childhood"[5] presents unprecedented risks from identity theft to psychological manipulation through targeted advertising, from algorithmic profiling to potential future discrimination based on digital histories and footprints as everything is now accessible on the internet and it also puts them at a risk of being quite vulnerable. The effectiveness of these protections will ultimately depend on regulatory vigilance, organizational compliance, and society's evolving understanding of childhood in an increasingly datafied world.

2. Core Principles of Child Data Protection

At the heart of the DPDP Act lies a protection framework with several key concepts and definitions of data fiduciaries, data principals, consent managers that play an essential role in Data protection. The principles and the definitions defined by the law in the act reflect a nuanced understanding that children require special protection while also respecting their evolving autonomy. At its core, the Act recognizes children as a distinct category of data principals and defines under section 2(6)[6] as "personal data" expansively to include any information related to an identified or identifiable natural person, which in the context of children encompasses not only basic identifiers such as names and photographs but also behavioral patterns, preferences, and digital footprints generated through various interactions. This raises a lot of ethical questions Firstly, what is the data retention period in this case? Secondly, who is the consent manager in case of children? Thirdly, what are the compliance requirements that are to be followed by Data Fiduciaries? And lastly, how will the parental consent be verified?

The DPDP Act and Rules don't just stand alone in regard to the safety of the children. It complements existing regulations such as protections provided under the Juvenile Justice Act 2015[7], POCSO Act 2012[8], and Information Technology Act 2000[9]. This legislative convergence creates a multidimensional protective framework addressing

5 CORE, https://core-evidence.eu/posts/how-does-the-collection-of-children-s-data-affect-privacy, (last visited Apr. 8, 2025)

6 Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 2(6), (India).

7 Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India).

8 Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).

9 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

varied aspects of children's digital vulnerabilities from exposure to harmful content to exploitation through commercial data practices. The interoperability of these legal instruments reflects the legislature's recognition that comprehensive protection requires addressing both content-based and data-processing risks that children face in contemporary digital environments. Together in a combination, these laws create a multi-layered shield addressing different dimensions of children's digital vulnerabilities that need to be addressed from explicit content to exploitative commercial practices After all we need to protect them at all cost.

3. Consolidated Parental Consent and Compliance Framework

3.1 Parental Consent and Age Verification Requirements: The cornerstone of child data protection under the DPDP Act lies in the comprehensive parental consent and verification framework established under Section 9 of the DPDP Act and Rule 10 of the Draft Rules. This framework goes beyond procedural checkboxes to create meaningful protection through systematic requirements that organizations must integrate into their operations, culture, and technical infrastructure.

3.2 Age Threshold and Consent Requirements: Unlike the graduated age models employed by GDPR (16 years, reducible to 13) and COPPA (under 13 years), India's DPDP Act establishes a uniform age threshold of under 18 years for all children requiring parental consent. This approach reflects India's commitment to providing comprehensive protection for all minors without age-based distinctions within the childhood category.

3.3 Verification Methods and Technical Implementation: The Rules outline specific technical and organizational measures that data fiduciaries must implement to verify that the consenting individual is indeed an adult parent or guardian of the minor child. This verification can be accomplished through two primary methods:

a. Existing Verified Information Route: Checking reliable identity details such as age information that are already available with the data fiduciary

b. Government-Authorized Verification Route: Through voluntarily provided identity details or virtual tokens issued by government-authorized entities, including Digital Locker service providers

3.4 Documentation and Record-Keeping Requirements: Data fiduciaries must maintain comprehensive records of their verification processes, consent mechanisms, and processing activities involving children's data as the data here is quite sensitive in nature and needs to be treated as such. This includes:

a. Documentation of how they determine and verify parental status

b. Implementation of age verification protocols

c. Compliance records with prohibitions on harmful processing

d. Specification of how Digital Lockers function in verification processes

e. Records must be available for regulatory inspection and demonstrate ongoing compliance with both the Act and Rules

3.5 Data Retention and Deletion Protocols: Under the DPDP Act and Rules, specific retention periods are established for different sectors. For social media platforms with large user bases and online gaming intermediaries - the two sectors most relevant to children - the following requirements apply:

a. Data fiduciaries must retain children's data only for the period necessary to fulfil the purpose for which it was initially collected

b. Maximum retention period of three years from the last user interaction

c. 48-hour notification requirement before permanent deletion of personal data

d. Mandatory data erasure once the purpose is served or the retention period expires

3.6 Compliance Paradigm Shift: These consolidated requirements represent a paradigm shift in how organizations must approach children's data protection. Rather than treating children's data as an afterthought, the DPDP framework requires organizations to fundamentally redesign their data processing systems with children's protection as the heart and soul of its values, supported by robust verification mechanisms and clear prohibitions on harmful practices.

4. Global Framework: The story of GDPR and COPPA

The Digital Personal Data Protection Act of India emerges within an established international regulatory landscape. Two frameworks have been particularly influential in shaping global approaches to children's data protection: the European Union's General Data Protection Regulation[10] (herein after referred to as "GDPR") and the United States' Children's Online Privacy Protection Act (herein after referred to as "COPPA")[11]. Each represents distinct regulatory philosophies while pursuing common protective objectives that is children's digital privacy in the current age and time. Analysing these frameworks provides essential context for understanding India's approach under the DPDP Act.

4.1 The European Approach: GDPR's Child Protection Framework

The GDPR[12] explicitly recognizes children as deserving "specific protection" regarding their data, acknowledging their particular vulnerability to commercial exploitation and limited capacity to recognize privacy risks. This recognition materializes through several key provisions:

The GDPR establishes a graduated consent model based on age thresholds. Article 8[13] sets *sixteen years* as the default age of digital consent, though Member States retain discretion to lower this threshold to even *thirteen years*. For children below the applicable age threshold, the processing of personal data requires verifiable consent from the holder of parental responsibility. Additionally, the Regulation requires that consent requests directed at children be formulated in clear, age-appropriate language that facilitates genuine understanding.

Beyond consent requirements, the GDPR implements substantive protections for children's data. Article 35[14] necessitates data protection impact assessments for processing operations likely to present high risks to children's rights and freedoms.

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1.

11 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2018).

12 *supra* note 11 at page 4.

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 8, 2016 O.J. (L 119) 1, 53.

14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 35, 2016 O.J. (L 119) 1, 53.

Article 22[15] contains provisions restricting automated decision-making that produces legal or similarly significant effects concerning children. Article 17's[16] "right to be forgotten" acquires heightened significance for data collected during childhood, reflecting the Regulation's recognition that children may not fully comprehend the future implications of their digital footprint. Finally, Article 12[17] mandates that privacy notices addressed to children employ clear, plain language appropriate to their comprehension level.

4.2 The American Approach: COPPA's Protective Framework

The Children's Online Privacy Protection Act of 1998[18] represents the United States' primary legislative response to children's digital privacy concerns. Unlike the GDPR's broader scope, COPPA specifically targets online services directed at or knowingly collecting information from children under *thirteen* years of age.

COPPA establishes stringent consent and verification requirements. The Act prohibits the collection of personal information from children without obtaining verifiable parental consent through methods specified by the Federal Trade Commission. These methods include credit card verification, signed forms, video identification, and knowledge-based authentication protocols. COPPA also grants parents the right to review information collected from their children and request its deletion, establishing a continuing parental oversight mechanism.

The Act further imposes specific operational requirements on covered entities. These include mandates for privacy notices specifically designed for children's services, substantive restrictions on the categories of personal information that may be collected, and significant limitations on behavioral targeting and profiling of children for advertising purposes. These requirements reflect COPPA's foundational concern with preventing exploitative commercial practices directed at children.

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 22, 2016 O.J. (L 119) 1, 53.

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 17, 2016 O.J. (L 119) 1, 53.

17 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 12, 2016 O.J. (L 119) 1, 53.

18 *supra* note 12 at page 4.

Table 1: Comparative Analysis with DPDP

Aspect	GDPR (EU)	COPPA (US)	DPDP (INDIA)
Age	16 years (but can be lowered to 13 by member states)	Under 13 years	Under 18 years
Consent Requirements	Parental consent required for information society services. Must be "verifiable" and specific	Verifiable parental consent required before collecting or using children's personal information	Verifiable parental consent mandatory through technical and organizational measures. Specific verification methods including Digital Locker
Verification Methods	Methods for verification are not specifically prescribed herein.	Multiple acceptable methods: Credit card, government ID, video verification, knowledge-based questions	Two specific routes: Existing verified details with data fiduciary or government-authorized verification systems

5. AI And Children's Privacy: Emerging Challenges And Regulatory Responses

The rapid advancement of Artificial Intelligence (herein after referred to as "AI") technologies presents unique and complex challenges to children's privacy protection that extend beyond traditional data collection concerns and also beyond something that was initially . As AI systems increasingly permeate educational technologies, gaming platforms, social media, and even toys, they create unprecedented risks to children's data rights that the DPDP framework must address.

5.1 AI-Powered Data Processing: Beyond Simple Collection

AI systems fundamentally transform how children's data is processed by enabling sophisticated analytics that can infer sensitive information even from seemingly innocuous data points[19]. These systems can create detailed behavioral

19 Lupton, D., & Williamson, B. (2022), *The datafied child: The dataveillance of children and implications*

profiles, predict preferences, and even assess psychological states through pattern recognition techniques that children and parents may not fully comprehend. Under the DPDP Act, this raises critical questions about whether standard parental consent mechanisms are sufficient when the implications of AI processing extend far beyond what is initially apparent at collection.

The Act's provisions requiring data fiduciaries to implement age-appropriate design principles become particularly significant in AI contexts, as such systems must be designed with constraints that prevent excessive profiling of minors, regardless of whether technical consent requirements have been satisfied[20]. The prohibition on processing that could cause "significant harm" to children takes on new dimensions when AI systems can make automated decisions affecting educational opportunities, content exposure, and social interactions.

5.2 AI-Enhanced Platforms and Algorithmic Amplification

Social media platforms and gaming environments increasingly employ recommendation algorithms that can intensify children's vulnerability online. These systems, though initially designed to maximize engagement, may inadvertently expose children to inappropriate content or encourage excessive screen time through highly personalized content delivery, which can be a shortcoming to start with[21]. The DPDP Act's focus on preventing harmful processing must be interpreted to include algorithmic amplification that exploits children's developmental vulnerabilities, as they are highly perceptive to change and can be affected in either a positive or negative sense.

Data fiduciaries deploying AI systems must now consider how their algorithmic decision-making processes might affect children differently than they affect adults.

for their rights, NEW MEDIA & SOCIETY, 24(1), 1 16, https://journals.sagepub.com/doi/full/10.3102/01623737231202469?af=R&ai=1gvoi&mi=3ricys (last visited Apr. 8, 2025)

20 Livingstone, S., Stoilova, M., & Nandagiri, R. (2023). "Children's data and privacy online: Growing up in a digital age." Policy Press, https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf, (last visited Apr. 8, 2025).

Livingstone, S., Stoilova, M., & Nandagiri, R. (2023), *Children's data and privacy online: Growing up in a digital age,* POLICY PRESS, https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf, (last visited Apr. 8, 2025).

21 Keller, D., & Leerssen, P. (2022), *Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation,* In N. Persily & J. Tucker (Eds.), Social Media and Democracy, Cambridge University Press, https://www.researchgate.net/publication/343996375_Facts_and_Where_to_Find_Them_Empirical_Research_on_Internet_Platforms_and_Content_Moderation , (last visited Apr. 8, 2025).

This may require specialized impact assessments for AI systems that interact with or process children's data, going beyond the general compliance requirements outlined in the Act. For instance, AI systems used in educational technology must be designed to prioritize pedagogical benefits over data extraction, with appropriate safeguards in place to prevent profiling that could lead to discriminatory outcomes.

5.3 Voice Assistants, Smart Toys, and Ambient Intelligence

The proliferation of voice-activated devices, smart toys, and IoT products designed for children creates ambient data collection environments that challenge traditional notice and consent frameworks. These technologies often collect biometric data (voice patterns), location information, and behavioral data continuously and passively. Under the DPDP framework, such technologies must implement particularly robust verification mechanisms and clearly delineate how AI processing of such intimate data complies with the principle of data minimization[22].

Smart toys that employ AI to "learn" from interactions with children present a regulatory challenge that straddles privacy and product safety concerns[23]. The DPDP Act's requirements for verifiable parental consent must be adapted to these contexts where data collection is ongoing rather than discrete, and where AI processing continuously evolves based on interaction patterns.

5.4 Comparative Regulatory Approaches to AI and Children's Privacy

While India's DPDP Act establishes a baseline for protection, other jurisdictions have developed more specific guidance for AI systems processing children's data, like the EU's AI Act classifies AI systems used with children as "high-risk"[24] applications requiring rigorous assessment protocols and transparency requirements that exceed standard GDPR provisions. Moreover, the United Kingdom's Age-Appropriate Design Code specifically addresses automated profiling and decision-making for children's services, requiring that profiling be switched off by default for child users and lastly, California's Age-Appropriate Design Code Act of 2022 requires businesses to complete Data Protection Impact Assessments that specifically evaluate

22 Berman, G., & Carter, K. (2018), *Children's Privacy in the Big Data Era: Research Opportunities,* UNICEF Office of Research-Innocenti, Research Brief 2018-19. https://www.unicef-irc.org/publications/pdf/IRB_2018-19.pdf, (last visited Apr. 8, 2025).

23 Federal Trade Commission. (2023). *Protecting Kids from Stealth Advertising in Digital Media*, FTC Policy Statement. https://www.ftc.gov/system/files/ftc_gov/pdf/p064504kiddigitaladsstatement.pdf, (last visited Apr. 8, 2025).

24 *Ibid.*

how AI systems might harm children through profiling or behavior manipulation. India's regulatory framework would benefit from similar AI-specific provisions that recognize the unique risks posed by these technologies to children's developing autonomy and privacy rights.

5.5 Required Safeguards for AI Systems Processing Children's Data

To effectively protect children in AI-driven environments, data fiduciaries under the DPDP Act should implement:

a. Algorithmic accountability measures that make AI decision-making explainable in age-appropriate terms to each and every one, or in layman terms to make it more accessible and user friendly[25].

b. Regular algorithmic audits to identify and mitigate bias or manipulation affecting child users and to keep a check if its being used maliciously.

c. Default settings that limit data processing to the minimum necessary for providing the service and to constantly have parental supervision.

d. Human oversight mechanisms for AI systems making consequential decisions affecting children and making sure that it isn't used in a manner that wasn't intended.

e. Technical limitations on inference generation from children's data

These safeguards would complement the existing DPDP framework by addressing the specific risks presented by AI technologies that may otherwise exploit loopholes in consent-based protection models[26].

The integration of AI-specific provisions into India's children's data protection framework represents the next frontier in safeguarding young digital citizens. As AI systems become increasingly sophisticated and ubiquitous, the DPDP Act's effectiveness will depend on how robustly it can be interpreted and enforced to address the unique challenges posed by artificial intelligence in children's digital environments.

25 U.N. Children's Fund, *Policy Guidance on AI for Children 2.0* (2021), https://www.unicef.org/innocenti/media/1341/file/UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021.pdf.

26 Derek E. Baird, *The Importance of Protecting Children's Rights and Data Privacy in the Age of AI*, Medium (Mar. 15, 2023), https://derekebaird.medium.com/the-importance-of-protecting-childrens-rights-and-data-privacy-in-the-age-of-ai-c154d22f9d0f.

6. AI AND EDTECH: THE NEED FOR TARGETED GOVERNANCE

One pressing area that requires further attention within the present framework is the rapid adoption of Artificial Intelligence (AI) in educational technology (EdTech) platforms. We hear so many times about the schools being held in virtual mode especially after the Covid Break and new AI tools being evolved and made for the rapid advancement of these platforms. But, While EdTech tools offer personalised learning experiences, they also gather sensitive data that may range from academic performance and attention metrics to biometric data such as facial expressions and voice patterns[27].

Although the DPDP Act provides a general prohibition on processing likely to cause harm and mandates age-appropriate design, these provisions may not sufficiently address the complexity of AI-powered data in educational settings. Verifiable consent, though mandated, is often impractical in real-time classroom environments. Additionally, ambiguity persists regarding whether schools or third-party vendors bear primary fiduciary responsibility in such contexts.

Globally, jurisdictions have begun to respond. The EU's AI Act[28] classifies AI used in education as "high-risk," necessitating strict transparency and risk assessment requirements[29]. Similarly, the UK's Age-Appropriate Design Code[30] mandates that profiling features be turned off by default for child users. India currently lacks equivalent, EdTech-specific AI regulations, are a gap that could undermine the spirit of the DPDP Act and that needs to be addressed effectively.

As education is not merely transactional but developmental, allowing opaque AI systems to shape what children see, learn, or are evaluated risks institutionalising bias and surveillance as we also need to understand that the technology we are building isn't just an innovation but a path towards changing the complete fundamental norms that we earlier relied on . There is a pressing need to introduce

27 Ben Williamson & Anna Hogan, *Commercialisation and Personalisation in Education: A Critical Survey of Data and EdTech,* 38 LEARNING, MEDIA & TECHNOL. 254 (2020).

28 U.S. Dep't of Educ., Off. of Educ. Tech., *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations* (May 2023), https://www.ed.gov/sites/ed/files/documents/ai-report/ai-report.pdf.

29 EUROPEAN PARLIAMENT, EU AI Act: First Regulation on Artificial Intelligence, Eur. Parl. (June 1, 2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

30 UK INFORMATION COMMISSIONER'S OFFICE, Age Appropriate Design Code (Children's Code) (Sept. 2, 2020), https://ico.org.uk/for-organisations/childrens-code/

AI governance guidelines that mandate:

a. Transparent and explainable algorithms,

b. Mandatory algorithmic audits for bias and manipulation,

c. Data minimisation protocols tailored to learning environments,

d. Clear division of fiduciary responsibility between schools and vendors,

e. Human oversight in any AI-led decision-making impacting a child.

Such provisions would reinforce the DPDP's child-centric principles and ensure that classrooms remain environments of empowerment not covert data extraction. The DPDP Act and Rules represent a critical evolution in India's privacy jurisprudence, even though they place children's rights at the centre of the data protection conversation but still there are certain fragments that need to be addressed. However, the rise of AI-powered tools, particularly in education, reveals new and complex challenges, challenges that weren't exactly thought of before but exist now. To stay ahead of emerging threats, India's data protection regime must not only enforce compliance with existing provisions but also anticipate future risks by developing domain-specific policies especially in AI and EdTech. Doing so will ensure that the promise of digital empowerment does not come at the cost of children's dignity, autonomy, or future.

7. Enforcement Mechanisms And Penalties

The matter of children privacy is quite sensitive in its own regards hence the penalties imposed on the data fiduciaries if found to be in violation of the compliance requirements are quite high in nature. The framework operates through the Data Protection Board of India, which serves as the primary enforcement authority with comprehensive powers to investigate, penalize, and ensure compliance with children's data protection requirements.

The Act aims to implement a stringent penalty structure for violations involving children's data, with financial penalties that may reach up to ₹250 crore[31] for serious breaches of children's data protection requirements and breach of data protection requirement in general as well. The quantum can increase based on various factors including the nature, gravity, and duration of the violation and how much effect it

31 Digital Personal Data Protection Act, 2023, No. 22, Section 33, Acts of Parliament, 2023 (India).

has had on the people.

For continued non-compliance, additional penalties of up to ₹20,000 per day may be imposed[32]. Beyond financial penalties, the Board can mandate operational restrictions, including temporary suspension of data processing activities or permanent prohibition from processing children's data, along with requirements for third-party audits and system modifications.

Organizations that maybe found in violation face immediate compliance requirements and must implement long-term remedial measures. Immediate actions may include ceasing non-compliant processing, notifying affected parties, implementing corrective measures, and submitting detailed compliance reports. Long-term measures require organizations to enhance their security systems, update verification mechanisms, revise internal policies, and conduct regular audits to prevent future violations.

This enforcement regime under the DPDP Act represents one of the most stringent frameworks globally for protecting children's digital privacy. By combining substantial penalties with comprehensive oversight and remedial requirements, it creates a regulatory environment that prioritizes the protection of children's personal data and incentivizes organizations to implement robust safeguards. The framework's effectiveness will largely depend on the Data Protection Board's vigilance and the willingness of organizations to invest in comprehensive compliance measures.

8. Case Studies

There are various case studies presenting the blatant violation of the personal data privacy rights of the children in India and around the globe and as the result of the same fines have been imposed on the data fiduciaries. Some of the relevant case studies are:

The *Aradhya Bachchan case*[33] who at the time was merely 11 years of age, sued YouTube and Google LLC in the courts of India when her privacy was severely

32 Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

33 Aishwarya Rai Bachchan v. Google LLC, Delhi High Court Issues Notice to Online Platforms Over Fake Videos of Aaradhya Bachchan, India Today (Feb. 3, 2025), https://www.indiatoday.in/india/law-news/story/aaradhya-bachchan-delhi-high-court-fake-videos-online-platforms-google-notice-2674174-2025-02-03, (last visited Apr. 15, 2025).

violated and discarded for as some of the media outlets were circulating false images and news claiming that she was critically ill or dead. The Delhi High Court in this matter stepped forward and ordered Google LLC to take down such news and the importance of safeguarding children's privacy emphasised more.

In Sweden, the Swedish Data Protection Authority[34] fined SEK 200,000 on the Secondary education Board in Skelleftea municipality as they used facial recognition technology over three weeks in order to monitor 22 Secondary School students hampering and violating their privacy in the process.

In a study[35] it was found that Google, Facebook skimmed most of their data from apps meant for kids, with Google being the highest recipient at collecting 33% of the data collected from such apps, followed by Facebook at 22%, as per the study that covered 60 children's Android applications across nine categories including games, edtech, school, coding, and childcare.

Last year, in 2024 Microsoft[36] was found in the violation of the privacy rights of the children with its software of Microsoft 365 and the complaint was filed against it. The Big-tech company blamed schools for this violation.

9. CONCLUSION

The Digital Personal Data Protection Act and Rules mark a significant milestone in India's approach to protecting children's digital privacy rights. The questions are just merely questions but should be thought provoking as privacy is something really important in today's world, with every personal and intimate movement of individuals being online ready to be exploited. By establishing comprehensive compliance requirements, such as verification mechanisms, and stringent penalties, the framework would create a robust system for safeguarding children's personal data, which is a huge step forward towards a safer environment where the online presence isn't hampered but protected at all costs. The new legislations draw

34 (2019) 'Facial Recognition: School ID checks lead to GDPR fine', BBC News, August. Available at: https://www.bbc.com/news/technology-49489154 (last visited Apr. 15, 2025).

35 The Economic Times (2023) 'Google, Facebook skim most data from apps for kids: study', The Economic Times, https://economictimes.indiatimes.com/tech/technology/google-facebook-skim-most-data-from-apps-for-kids-study/articleshow/107209705.cms (last visited Apr. 15, 2025).

36 The Cyber Express (n.d.) 'European Center for Digital Rights Microsoft', The Cyber Express. Available at: https://thecyberexpress.com/european-center-for-digital-rights-microsoft/ (last visited Apr. 15, 2025).

their inspiration from global frameworks like GDPR and COPPA while adapting to India's unique digital landscape, particularly through innovations like Digital Locker integration for parental consent verification and virtual tokens which again would be game changer in its own way.

Recent case studies, from the Aradhya Bachchan incident to violations by tech giants like Google and Microsoft, underscore the pressing need for such protective measures as our children are the future of tomorrow. The Act's enforcement mechanisms, including penalties up to ₹250 crore and daily fines for continued non-compliance, demonstrate India's serious commitment to protecting its youngest digital citizens. As technology continues to evolve, this legislative framework provides a foundation for ensuring that children's privacy rights remain protected in an increasingly digital world.