Cognitive Thinking: An International Journal of Interdisciplinary Studies
Vol. 2, Issue-2 (April-June, 2026), pp.192-204, ISSN: 3107-5088, www.cognitivethinking.in

Role of Artificial Intelligence in Child Development: A Legal Perspective

Babita Pathak
LL.M., 247/PLL/005
School of Law, Justice & Governance, Gautam Buddha University, Greater Noida (U. P.)
Email: babita92111@gmail.com

Dr. Santosh Kumar Tiwari
Assistant Professor
School of Law, Justice & Governance, Gautam Buddha University, Greater Noida (U.P.)
Email: santoshtiwari@gbu.ac.in

Article: Received: 22/05/2026, Returned: 28/05/2026, Accepted: 04/06/2026, Published:06/06/2026.
D.O.I. https://doi.org/10.5281/zenodo.20563963

Abstract: AI (artificial intelligence) is becoming ubiquitous in many areas of child development: education, health care, entertainment, and social interaction. The ability to use AI tools to provide customized education, quickly identify developmental disabilities, and improve security will have an unprecedented impact on how children develop physically, emotionally, socially, and cognitively. However, AI presents legal and ethical challenges that have never been encountered before. This paper reviews the impact of AI on child development according to law in India by looking at Indian law and other countries' laws, with particular emphasis on the General Data Protection Regulation (GDPR), the United Nations Convention on the Rights of the Child (UNCRC), as well as new AI laws being implemented in the EU and US. The research identifies key areas of legal limitations in India regarding algorithmic accountability, data protection of children, informed consent in AI environments, and liability for developmental harms caused by AI. The paper concludes with policy recommendations to harmonize AI innovation with child rights and developmental justice.
Keywords: *Artificial Intelligence, Child Development, Data Protection, DPDP Act 2023, Algorithmic Accountability, Child Rights, Legal Liability*

1. Introduction: There has been a significant increase in the amount of Artificial Intelligence being utilized by children. From educational apps with Artificial Intelligence, like Byju's and Khan Academy, to voice assistants, like Amazon's Alexa and Google's, to recommendation algorithms for kids on Youtube, to AI Mental Health Chatbots for teenagers, children are increasingly interacting with these systems that use machine learning and have an effect on their behaviour.[1] According to the United Nations' UNICEF, AI systems are now in deployment in over 100 countries to promote child welfare and support child education and child healthcare.[2]However, the same algorithms that create personalized

[1]UNICEF, *Policy Guidance on AI for Children* (2021) 5, https://www.unicef.org/globalinsight/media/2356/file/UNICEF-Global-Insight-policy-guidance-AI-children-2021.pdf.
[2]UNICEF, *Artificial Intelligence and Children's Rights: A Policy Guide* (2020) 3.

learning experiences also create bias and collect sensitive personal behaviour information without meaningful consent and expose children to potentially harmful or manipulative content.[3]

The primary legal question, therefore, is whether our existing government frameworks for protecting children that are designed for the analog world can also protect children from the unique threats posed by AI systems. In India, the laws addressing the protection of children, like the Juvenile Justice (Care and Protection of Children) Act 2015, the Information Technology Act 2000, and the newly released Digital Personal Data Protection Act 2023 (DPDP Act), do provide some guidance on preventing these harms to children through the use of Children's Technology, but none specifically address the long-term developmental effects of these types of decisions created through an algorithm.[4]

2. Conceptual Framework: AI in Child Development

2.1 Defining Artificial Intelligence

An AI system can be defined legally as a system that analyses its surroundings and performs actions autonomously to reach set goals that exhibit intelligent behaviour.[5]As per the OECD definition, defined by human objectives, an AI system is a machine-based system that can make predictions about real/virtual environments as well as; recommendations/decisions."[6]

2.2 Applications of AI in Child Development

AI affects child development across multiple domains:

Education: AI is widely utilized in the education sector by adaptive learning platforms, which can evaluate a student's knowledge at the beginning of their learning and custom fit education based on that level. Intelligent tutoring systems supply instant feedback as students complete their work. AI has also been used to help monitor student activity during virtual exam/assessment environments using proctoring tools.[7]

Healthcare: AI-enabled tools that assess whether a patient may develop autism spectrum disorder, ADHD, and speech disorders are all examples of how AI is being used in healthcare to identify conditions sooner. Adolescents will benefit from the support of chatbots that deliver mental health advice. A variety of wearable/monitoring devices can be used to monitor physiological data.[8]

Entertainment and Social Interaction: In terms of entertainment and social interaction, recommendation algorithms used on YouTube Kids, TikTok, and Instagram help determine what people watch or read online. AI-created friends (like Replika) and social robots (such as Moxie) simulate human interaction.[9]

Safety and Protection: AI systems provide safety and security solutions, like content filtering, detecting cyberbullying, identifying grooming, and locating missing children using facial recognition technology.[10]

2.3 Developmental Vulnerabilities

[3]S. Livingstone & M. Stoilova, *The 4Cs of Online Risk: Classification Framework*, London School of Economics (2021) 12–15.
[4]N. Jain & P. Reddy, "Regulating AI in India: The Missing Framework for Child Protection," (2023) 8(2) *Indian Journal of Law and Technology* 45, 52.
[5]European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence* (AI Act), COM(2021) 206 final, Article 3(1).
[6]OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2019) para 1.2.
[7]K. Chaudhary, "AI in Indian Classrooms: Promises and Perils," (2022) 14(3) *Journal of Educational Technology & Society* 78, 82.
[8]World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (2021) 34–36.
[9]M. Hicks, "Algorithmic Curation and Child Development," (2023) 45(1) *New Media & Society* 112, 120.
[10]INTERPOL, *AI and Child Safety: A Review of Current Applications* (2022) 8–10.

Children are not tiny versions of adults. Their social, emotional, and cognitive abilities are still immature. Every child goes through four developmental phases, according to Jean Piaget's theory: sensorimotor (birth to 2 years), preoperational (2 to 7 years), concrete operational (7 to 11 years), and formal operational (11 years and above). The stages are vulnerable to AI systems in different ways.

Young children may misplace their trust and attachment as they lack the metacognitive ability to differentiate a human from an artificially smart agent.[11]Adolescents are more technologically savvy but are also vulnerable to algorithmic manipulation, social comparison, and the collection of personal data.[12] From a legal perspective, these developmental vulnerabilities necessitate a higher standard of protectiona principle recognized in the UNCRC, which mandates that "in all actions concerning children, the best interests of the child shall be a primary consideration."[13]

3. Legal Framework in India

3.1 Constitutional Foundation

The Constitution of India does not explicitly mention AI or children's digital rights. However, several provisions are relevant:

Article 21 guarantees the right to life and personal liberty, which the Supreme Court has broadly interpreted to also encompass the right to privacy.,[14] the right to education,[15] and the right to health.[16] By extension, the right to be free from algorithmic harm could be argued as a facet of Article 21.

Article 21A establishes that children between the ages of six and fourteen have a basic right to free and compulsory education. If AI systems are deployed in schools, their design and functioning must not impede this right.

Article 15(3) allows the State to provide women and children with specific provisions. Affirmative regulation of AI systems that target children can be justified by this enabling provision.

Directive Principles under Articles 39(e) and 39(f), direct the State to protect children from abuse and provide them with opportunities for healthy growth and development.[17]

3.2 Juvenile Justice (Care and Protection of Children) Act, 2015

The JJ Act, 2015 defines a "child in need of care and protection" to include those who are "mentally or physically challenged or ill children or children suffering from terminal diseases or incurable diseases having no one to support or look after."[18] While not explicitly addressing AI, the Act's framework could extend to children harmed by algorithmic systemsfor example, a child developing an eating disorder due to AI-recommended thin-ideal content.

The Act also mandates the creation of Child Welfare Committees (CWCs) with powers to pass orders regarding the care and protection of children.[19] However, these bodies lack technical expertise in AI systems.

3.3 Information Technology Act, 2000 (as amended)

The IT Act, 2000 remains the primary cyber law in India. Key provisions include:

Section 67B prohibits publishing or transmitting material depicting children engaging in sexually explicit acts. AI-generated CSAM is included in the ban. However, the law is difficult to enforce.[20]

---

[11]S. Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other* (Basic Books, 2011) 87–90.
[12]Common Sense Media, *Teens and AI: Perceptions and Vulnerabilities* (2023) 15.
[13]UN Convention on the Rights of the Child, adopted 20 November 1989, 1577 UNTS 3, Article 3(1).
[14]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, para 169 (per Chandrachud J.).
[15]*Unni Krishnan, J.P. v. State of Andhra Pradesh*, (1993) 1 SCC 645, para 74.
[16]*State of Punjab v. Mohinder Singh Chawla*, (1997) 2 SCC 83, para 9.
[17]Constitution of India, Articles 39(e), 39(f).
[18]Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2 of 2016, § 2(14)(vi).
[19]Ibid., § 27.

Section 69 permits surveillance and scanning of data to identify AI systems with a risk of developmental harm but the procedural safeguards provided under this provision are weak.
Section 79 protects intermediaries where third-party content is posted on the service provided the intermediary has exercised due diligence. It is unclear whether AI-generated content produced by an algorithm rather than by an user may fall outside of Section 79's immunity, as Indian courts have not yet decided this question.[21]

3.4 Digital Personal Data Protection Act, 2023 (DPDP Act)

The DPDP Act, 2023 is India's first comprehensive data protection legislation. Several provisions are particularly relevant to children and AI:
Section 9 imposes special obligations when processing personal data of children. A Data Fiduciary (the entity determining the purpose and means of processing) must:

- Obtain verifiable consent of the parent or lawful guardian
- Not undertake processing that is likely to cause any detrimental effect on the well-being of the child
- Not undertake tracking or behavioral monitoring of children
- Not engage in targeted advertising directed at children[22]

The Act defines a "child" as an individual who has not completed the age of 18 years. This uniform age threshold is higher than many international frameworks (GDPR uses 13–16 years depending on Member State) but may be impractical for adolescents capable of limited independent decision-making.
Section 10 requires Significant Data Fiduciaries (SDFs)entities with larger volumes of data or higher riskto appoint a Data Protection Officer and conduct Data Protection Impact Assessments (DPIAs). Any AI system processing child data likely triggers SDF status.
Section 8 outlines the rights of the Data Principal (the child in this context), including the right to correction, erasure, and grievance redressal. However, these rights are exercisable through the parent or guardian, potentially silencing older children with genuine grievances.

Critical Gaps in the DPDP Act vis-à-vis AI:

The Act does not define "algorithm," "AI system," or "automated decision-making."
There is no provision for a right to explanation when an AI system makes a decision affecting a child.
The Act does not address the unique challenges of AI-generated synthetic data about children.
Enforcement mechanisms are untested, with the Data Protection Board yet to become fully operational.[23]

3.5 National Education Policy (NEP) 2020

The NEP 2020 acknowledges the impact of technology and artificial intelligence in education. According to paragraph 24.4 “AI-enabled personalised learning can help close the gaps in learning and provide tailored content.” The policy does not cover legal protection, data protection, or algorithmic accountability at EdTech platforms."[24]

3.6 Case Law Developments

Recent developments in Courts in India have involved litigation involving technology-child interaction; however, there is limited case law on the use of AI in education, specifically.

---

[20]Information Technology Act, 2000, No. 21 of 2000, § 67B.
[21]*Shreya Singhal v. Union of India*, (2015) 5 SCC 1, para 91 (discussing intermediary liability under Section 79).
[22]Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 9.
[23]Centre for Internet and Society, *The DPDP Act, 2023: A Critical Analysis* (2023) 22.
[24]Ministry of Education, *National Education Policy 2020* (Government of India, 2020) para 24.4.

***Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)** – Retired Justice K.S. Puttaswamy v. Union of India (2017): The Supreme Court ruled that Article 21 protects the right to privacy as a fundamental right. Although this case primarily involved the Aadhaar Scheme, Justice K.S. Puttaswamy's concurring opinion highlighted that privacy is "the constitutional core of human dignity" and that "digital surveillance may potentially chill the exercise of fundamental freedoms."[25]This logic applies directly to children in schools being subject to AI surveillance.

***X v. Union of India* (2021)** – The Delhi High Court considered the use of AI proctoring for university examinations during COVID-19. The Court held that all AI-based monitoring used for this purpose must be "proportionate, transparent, and have sufficient safeguards in place to ensure that data protection is adequate.[26]Although this case involved university students (adults), the reasoning in this case can be applied to children.

***Patanjali Ayurved Ltd. v. Twitchy Thought Pvt. Ltd*. (2022)** – The Delhi High Court recognised that the use of AI-generated content may damage reputations; however, the Court could not find that this created liability on the part of the AI developer.[27]Therefore, there is currently no answer to the question of whether an AI developer has civil liability for harm caused to the child development of children.

4. International Legal Instruments

4.1 United Nations Convention on the Rights of the Child (UNCRC)

The UNCRC (1989) stands as the most universally endorsed human rights treaty ever. India ratified this treaty in 1992. Important clauses related to AI are:

Article 3: "In every action concerning children, the best interests of the child must be a primary consideration." This principle ought to direct the design, implementation, and regulation of AI systems that interact with children.

Article 12: Children have the right to freely express their opinions in all matters that impact them. AI systems that restrict children's autonomy or influence their decisions breach this right.

Article 16: No child shall face arbitrary or unlawful infringements on their privacy. AI-driven tracking and surveillance of children clearly engages this article

Article 17: Countries that are parties recognize the significant role that mass media plays and shall guarantee that children have access to information from a wide range of sources. AI-driven content systems that frequently generate filter bubbles could be at odds with this requirement.

General Comment No. 25 (2021) on children's rights in the context of the digital environment was endorsed by the UN Committee on the Rights of the Child. The Comment explicitly states that "the design, implementation, and regulation of artificial intelligence systems must be guided by the best interests of the child."[28] It further requires states to ensure that AI systems used for child-related purposes are subject to independent, child-rights-based impact assessments.

4.2 General Data Protection Regulation (GDPR) (EU)

The GDPR contains several provisions specifically protecting children:

Recital 38 states that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned."[29]

---

[25]*Puttaswamy*, (2017) 10 SCC 1, para 616 (Kaul J., concurring).
[26]*X v. Union of India*, 2021 SCC OnLine Del 5120, para 23.
[27]*Patanjali Ayurved Ltd. v. Twitchy Thought Pvt. Ltd.*, 2022 SCC OnLine Del 4872, para 15.
[28]UN Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc CRC/C/GC/25, para 94.
[29]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 (General Data Protection Regulation) [2016] OJ L119/1, Recital 38.

Article 6(1)(a) requires consent for data processing. For children below 16 years (or 13 years at Member State option), consent must be given or authorized by the holder of parental responsibility.[30]
Article 22 It gives people the right to be free from decisions made solely by automated processing, including profiling, when those judgments have a substantial influence on them or have legal ramifications. The "significantly affects" standard should be applied generally to youngsters.
Article 35 When data processing is likely to seriously jeopardize people's rights and liberties, it requires a Data Protection Impact Assessment (DPIA). The European Data Protection Board (EDPB) has specified that processing of child data for profiling or automated decision-making always requires a DPIA.[31]

4.3 Proposed EU AI Act (Adopted 2024)

The EU AI Act, which entered into force in August 2024, is the world's first comprehensive AI regulation. It adopts a risk-based approach:

- **Unacceptable risk** (prohibited): AI programs that use subliminal techniques to drastically alter a person's behavior in ways that could cause bodily or psychological harm, as well as programs that exploit children's vulnerabilities due to their age or disability.[32]
- **High risk** (regulated): AI systems used in education and vocational training (e.g., admission algorithms, placement tools, assessment systems); AI systems used in employment and worker management. These require conformity assessments and post-market monitoring.
- **Limited risk** (transparency obligations): Chatbots and emotion recognition systems must disclose their AI nature.

With few exceptions, the Act expressly forbids the use of AI for social scoring and real-time remote biometric identification in public areas.

4.4 United States Approach

The US lacks a comprehensive federal AI law. Instead, regulation is sectoral and state-driven:
Children's Online Privacy Protection Act (COPPA) (1998): Requires websites and online services that target children to receive verifiable parental consent from those responsible for children's online activity prior to collecting personal data about the child.[33]COPPA has been criticized for its limited coverage (does not protect children between the ages of 13 and 17) and for not addressing the unique risks associated with artificial intelligence.[34]
California Consumer Privacy Act (CCPA), Provides minors ages 13 to 16 with the ability to opt in to having their personal data collected. For those under 13, the only way to collect personal data is by obtaining verifiable parental consent.[35]
Algorithmic Accountability Act (proposed): Would require organizations to conduct assessments of the algorithms they create for bias, establish privacy risks, and have a primary focus on how they may

[30]Ibid., Article 6(1)(a), Article 8(1).
[31]European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (2020) para 3.2.
[32]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (EU AI Act) [2024] OJ L, Article 5(1)(a)–(b).
[33]Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505 (2013).
[34]S. Mintz, "COPPA at 25: Rethinking Child Online Privacy in the Age of AI," (2023) 47 *Harvard Journal of Law & Public Policy* 1, 25.
[35]California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199, § 1798.120(b)–(c) (amended by CPRA 2020).

affect children, due to the increasing use of artificial intelligence tools. As of 2024, the bill has yet to be approved by Congress.[36]

4.5 Other Jurisdictions

China – The Online Protection of Minors' Personal Data Regulation (2019) requires separate parental consent for processing child data and prohibits algorithms from pushing addictive content to minors. The Algorithmic Recommendation Regulation (2022) requires AI recommendation systems to provide a mechanism for users to turn off personalized recommendations.[37]

Singapore – The Personal Data Protection Act (PDPA) does not have specific child provisions, but the Personal Data Protection Commission has issued guidelines recommending enhanced protection for child data.[38]

5. Liability for AI-Caused Developmental Harm

5.1 The Liability Gap

When an AI system causes developmental harm to a childfor example, an AI tutor that reinforces a learning disability, a mental health chatbot that gives dangerous advice, or a recommendation algorithm that pushes self-harm contentthe question arises: who is legally liable?

Traditional tort law requires a plaintiff to prove duty, breach, causation, and damages.[39] In AI contexts, each element presents challenges:

Duty: Did the AI developer, deployer, or user owe a duty of care to the child? Indian courts have recognized a duty of care in product liability cases,[40] but AI systems are not static "products"they evolve through machine learning.

Breach: What constitutes a breach of duty for an AI system? The standard of care might be that of a "reasonable AI developer," but no such standard has been judicially articulated.

Causation: Demonstrating that the AI's specific outputrather than other factors (family environment, peer influences, other technologies) caused the developmental harm is notoriously difficult. Developmental outcomes are multi-causal. [54]

Damages: How does one quantify developmental harm? Loss of educational attainment, psychological trauma, reduced future earning capacityall are challenging to measure and prove.

5.2 Theories of Liability

Several legal theories have been proposed to address this gap:

Product Liability: If an AI system is characterized as a product, the manufacturer could be held strictly liable for defects. The Consumer Protection Act, 2019 in India defines a "product liability action" as a claim against a product manufacturer for harm caused by a defective product. A "defect" includes any flaw in the product's design, manufacturing, or inadequate instructions. An AI system that poses unreasonable risks to children could be argued to have a design defect. However, the Act does not explicitly cover software or AI systems.

Negligence: A developer or deployer could be sued for negligence if they failed to exercise reasonable care in designing, testing, or monitoring the AI system. The landmark case of *Donoghue v. Stevenson* (1932) established the "neighbor principle"one must take reasonable care to avoid acts or

[36]Algorithmic Accountability Act of 2022, S. 3572, 117th Cong. (2022).
[37]Cyberspace Administration of China, *Provisions on the Administration of Algorithmic Recommendations in Internet Information Services* (2022), arts. 7, 12.
[38]Personal Data Protection Commission Singapore, *Advisory Guidelines on the Personal Data Protection Act for Children's Personal Data* (2022) para 2.1.
[39]Ratanlal&Dhirajlal, *The Law of Torts* (27th ed., LexisNexis, 2016) 45.
[40]*M.P. Electricity Board v. Shail Kumari*, (2002) 2 SCC 162, para 10.

omissions that could foreseeably injure one's neighbor.[41] An AI developer knows or should know that children will interact with their system, creating a foreseeable risk.

Vicarious Liability: The law may impose vicarious liability on an AI developer as if they are an agent or employee of the AI system if their actions are attributable to them as an agent. However, AI systems are generally not recognized as having legal personality, thus creating a conceptual challenge to this theory.[42]

Statutory Liability: A legislature can create a strict liability regime for damages caused by AI systems. The European Parliament has proposed an AI Liability Directive which is intended to simplify the ability for victims to receive damages from the companies that manufacture or sell AI systems; this will include changing the burdens of proof in certain situations. Currently, there is no law in India similar to this.[43]

5.3 Criminal Liability

Is it possible for an AI developer to face criminal liability for injury to child development? Under Indian Criminal Law, for most offences, the accused has mens rea (the intention to commit the offence).[44]The corporate entity has limited criminal liability, and further, is only held liable if it is established that its director or managers possessed the required mens rea.

In the event that an AI system that was developed and deployed was in fact tested, and did not meet acceptable standards, this gross negligence may be sufficient to charge the AI developer with Criminal Negligence under Section 304A (causing death by willful neglect) or Section 338 (causing serious bodily injury through a willful act that endangers human life or the safety of others) of the Indian Penal Code. However, to date, no Indian court has held that a company may be criminally liable for the actions of an AI system.

6. Policy Gaps and Regulatory Challenges

6.1 Absence of a Dedicated AI Legal Framework

India currently has no legislation specifically regulating artificial intelligence. The National Strategy for Artificial Intelligence (2018) and the Responsible AI framework (2021) published by NITI Aayog are policy documents without legal enforceability.[45] The proposed Digital India Act (still in draft as of 2024) is expected to address AI, but its provisions on child protection remain unclear.[46]

6.2 Informed Consent in AI Environments

The DPDP Act's requirement of "verifiable consent" of a parent or guardian for processing child data is conceptually sound but practically challenging. How does a platform verify that an adult providing consent is indeed the child's parent or guardian? The Act does not specify methods. Solutions such as government ID verification or biometric authentication raise their own privacy concerns.[47]

Moreover, the concept of "meaningful consent" breaks down when AI systems are complex and opaque. A parent cannot meaningfully consent to an AI system whose data practices are not fully transparent or whose future behavior cannot be predicted due to machine learning.[48]

6.3 Algorithmic Transparency and the "Black Box" Problem

---

[41] *Donoghue v. Stevenson* [1932] AC 562 (HL) 580 (per Lord Atkin).
[42] J. Guszcza, "The Last Mile of AI Liability," (2021) 33 *Stanford Technology Law Review* 421, 445.
[43] European Commission, *Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence* (AI Liability Directive), COM (2022) 496 final, Article 4.
[44] Indian Penal Code, 1860, No. 45 of 1860, § 40.
[45] NITI Aayog, *National Strategy for Artificial Intelligence* (2018); NITI Aayog, *Responsible AI for All* (2021).
[46] Ministry of Electronics & Information Technology, *Proposed Digital India Act* (Discussion Paper, 2023) Chapter 7.
[47] A. Sen, "Verifiable Parental Consent under the DPDP Act," (2023) 15 *NUJS Law Review* 301, 315.
[48] M. Kaminski, "The Right to Explanation, Explained," (2019) 34 *Berkeley Technology Law Journal* 189, 210–215.

Numerous AI systems utilise advanced concepts, resulting in being opaque to the supplier of the system and therefore creating issues around liability if something goes wrong, as there might be no firm, or anyone, who can explain how it made its decision and with whom liability lies. Moreover, as very few people (including developers) can provide an adequate explanation of how their AI system made a decision, it creates problems for courts in determining attribution of negligence.?[49]

Although some experts have called for an explanation, as referred to in Article 22 of the General Data Protection Regulation (GDPR), the question is whether it is technically achievable. The DPDP Act does not include an explanation.

6.4 Age Verification and Age Assurance

In order to provide child-specific protection to children, systems must identify children by the use of effective age verification of users. However, relying heavily on the upload of government issued documents is not a practical solution, as it carries with it the risk of breach of privacy and discrimination against the user. While the ability for children to self-declare themselves as a child includes the risk of being very easy to circumvent, there is currently no established national framework for the assurance of digital age of users in India.[50]

6.5 Enforcement and Remedy Mechanisms

In relation to the enforcement of existing laws, even when laws are in place, enforcement is weak. The Data Protection Board established by the DPDP Act has very limited investigative capabilities to conduct investigations into AI developments and therefore have no authority/ability to impose penalties. There are no specialist tribunals to deal with AI related child harms. Courts are inundated with work, and lack technical experience. As a result, there is likely to be considerable under-remedy for most of the harms experienced.[51]

6.6 International Coordination

AI systems can cross international borders. For example, a child in India may be harmed by an AI system that was developed in the US, stored/controlled by a company that is located in Germany, and/or was trained with data from various countries. Therefore, national regulations, which can only be applied within their jurisdictional territories, would not be sufficient to protect these kinds of violations or injuries. Although India is involved with the Global Partnership on Artificial Intelligence (GPAI), it is currently not a party to any binding international treaties relating to AI.[52]

7. Recommendations

7.1 Enact a Child-Centric AI Regulation

India should enact a dedicated legal framework for AI, with a specific chapter on child protection. This framework should:

- Prohibit AI systems that use subliminal techniques to manipulate children or that exploit child vulnerabilities.
- Classify AI systems used in education, healthcare, and child welfare as "high risk," requiring conformity assessments and ongoing monitoring.[53]
- Mandate child rights impact assessments for any AI system likely to interact with children.

7.2 Strengthen the DPDP Act for AI Contexts

The DPDP Act, 2023 should be amended to:

---

[49]F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015) 6–8.
[50]M. Gupta, "Age Assurance in India: Legal and Technical Challenges," (2023) 11 *Indian Journal of Data Protection* 45, 52.
[51]DPIIT, *Report of the Committee on Non-Personal Data Governance Framework* (2020) para 5.12.
[52]Global Partnership on AI, *Member Countries*, https://gpai.ai/members/ (last visited 20 May 2026).
[53]AI Act, supra note 42, Article 6, Annex III.

- Define "automated decision-making" and "algorithmic profiling" and provide children with a right not to be subject to solely automated decisions with significant effects.[71]
- Require Data Protection Impact Assessments specifically addressing AI risks to children.
- Provide for a right to meaningful explanation when an AI system makes a decision affecting a child.

7.3 Establish a Statutory Liability Regime

India should enact a statute creating strict liability for AI developers and deployers for developmental harm caused to children. The statute should:

- Reverse the burden of proof for causation where the AI system is opaque.[54]
- Allow for class action lawsuits on behalf of affected children.
- Establish a no-fault compensation fund for AI-related child harm, funded by contributions from AI developers.

7.4 Create Specialized Adjudicatory Mechanisms

The government should establish:

- A specialized tribunal within the National Human Rights Commission or the National Commission for Protection of Child Rights (NCPCR) to hear AI-related child harm cases.
- A technical expert panel to assist courts with evidentiary issues concerning AI systems.

7.5 Mandate Age Assurance and Child-Friendly Design

The Ministry of Electronics and Information Technology (MeitY) should issue binding rules requiring:

- Proportionate age assurance mechanisms for services likely to be accessed by children, balancing privacy with protection.
- "Child-friendly design" standards, including default high-privacy settings, transparent disclosures in age-appropriate language, and easy-to-use reporting mechanisms.

7.6 Integrate AI Literacy into Education

The NEP 2020 implementation should include:

- AI literacy as part of the school curriculum, teaching children how algorithms work, how data is collected, and how to exercise their rights.
- Training for teachers and parents on identifying and mitigating AI-related risks to children.

7.7 Pursue International Cooperation

India should actively participate in:

- Negotiations for a binding international treaty on AI and child rights, potentially under the auspices of UNESCO or the UN Human Rights Council.
- Bilateral and multilateral agreements for cross-border enforcement of judgments involving AI-caused child harm.

8. Conclusion

Children can benefit greatly from enhanced growth through the use of artificial intelligence, which will allow them to experience personalized learning, benefit from early health interventions, and ensure safety. However, with these possibilities also comes the possibility of significant legal and ethical risks to children. India currently has a patchwork, outdated legal system addressing these issues. Although there has been a recent step towards establishing some foundation with the introduction of the DPDP Act, 2023, this new legislation does not adequately address the unique features of AI systems; including opacity, autonomy, and continual evolution. In addition, neither the Juvenile Justice Act nor the IT Act anticipates machine learning and thus does not provide an adequate standard for liability when AI's potential to include child development is exploited in an unintended manner. Thus, this paper proposes

[54]cf. AI Liability Directive, supra note 58, Article 4.

that a comprehensive, child-centric legal framework balancing protection with innovation be established using the UNCRC as a foundation. This legal framework should include prohibitory measures for manipulative and exploitative AI, impact assessments, meaningful explanations of how an AI algorithm arrived to its conclusions, an adequate liability mechanism, and specialized enforcement measures. The urgency for these reforms cannot be overstated as children today are currently engaged in and involved with AI and will continue to be into the future as they grow up using AI in every facet of their daily life. Every day without an appropriate legal system in place is one more day that children can potentially encounter developmental harm without recourse. Law needs to evolve to keep pace with the rapid advancement of AI as technology continues to take hold not only on children, but on all humans.

Bibliography

Primary Sources

Statutes (India)

1. Constitution of India, 1950.
2. Consumer Protection Act, 2019 (No. 35 of 2019).
3. Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
4. Indian Penal Code, 1860 (No. 45 of 1860).
5. Information Technology Act, 2000 (No. 21 of 2000).
6. Juvenile Justice (Care and Protection of Children) Act, 2015 (No. 2 of 2016).
7. National Commission for Protection of Child Rights Act, 2005 (No. 4 of 2006).

Statutes (International)

8. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (USA).
9. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505 (USA).
10. Data Protection Act 2018, c. 12 (UK).
11. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ L 119/1 (2016).
12. Personal Data Protection Act 2012 (No. 26 of 2012) (Singapore).
13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (EU AI Act) [2024] OJ L.
14. Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 (USA).

Proposed Legislation

15. Algorithmic Accountability Act of 2022, S. 3572, 117th Cong. (2022) (USA).
16. Digital India Act (Discussion Paper), Ministry of Electronics & Information Technology, Government of India (2023).

Case Law

Indian Cases

17. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
18. *M.P. Electricity Board v. Shail Kumari*, (2002) 2 SCC 162.
19. *Patanjali Ayurved Ltd. v. Twitchy Thought Pvt. Ltd.*, 2022 SCC OnLine Del 4872.
20. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
21. *State of Punjab v. Mohinder Singh Chawla*, (1997) 2 SCC 83.
22. *Unni Krishnan, J.P. v. State of Andhra Pradesh*, (1993) 1 SCC 645.
23. *X v. Union of India*, 2021 SCC OnLine Del 5120.

International Cases

24. *Donoghue v. Stevenson* [1932] AC 562 (HL).

Treaties and International Instruments

25. APEC Privacy Framework, Asia-Pacific Economic Cooperation (2004, updated 2015).

26. UN Convention on the Rights of the Child, adopted 20 November 1989, 1577 UNTS 3.
27. UN Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc CRC/C/GC/25.

Government and Institutional Publications

28. Centre for Internet and Society. (2023). *The DPDP Act, 2023: A Critical Analysis*. Bengaluru: Centre for Internet and Society.
29. Cyberspace Administration of China. (2022). *Provisions on the Administration of Algorithmic Recommendations in Internet Information Services*.
30. Department for Promotion of Industry and Internal Trade (DPIIT). (2020). *Report of the Committee on Non-Personal Data Governance Framework*. New Delhi: Government of India.
31. European Commission. (2021). *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act)*, COM (2021) 206 final.
32. European Commission. (2022). *Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)*, COM (2022) 496 final.
33. European Data Protection Board. (2020). *Guidelines 3/2019 on processing of personal data through video devices* (Version 2.0).
34. European Data Protection Board. (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*.
35. INTERPOL. (2022). *AI and Child Safety: A Review of Current Applications*. Lyon: INTERPOL.
36. Ministry of Education, Government of India. (2020). *National Education Policy 2020*. New Delhi.
37. Ministry of Electronics & Information Technology, Government of India. (2023). *Proposed Digital India Act (Discussion Paper)*. New Delhi.
38. NITI Aayog, Government of India. (2018). *National Strategy for Artificial Intelligence*. New Delhi.
39. NITI Aayog, Government of India. (2021). *Responsible AI for All*. New Delhi.
40. OECD. (2019). *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449.
41. Personal Data Protection Commission Singapore. (2022). *Advisory Guidelines on the Personal Data Protection Act for Children's Personal Data*. Singapore.
42. UK Information Commissioner's Office. (2021). *Children's Code: Age-Appropriate Design Code*. London: ICO.
43. UNICEF. (2020). *Artificial Intelligence and Children's Rights: A Policy Guide*. New York: UNICEF.
44. UNICEF. (2021). *Policy Guidance on AI for Children*. New York: UNICEF Global Insight.
45. World Health Organization. (2021). *Ethics and Governance of Artificial Intelligence for Health*. Geneva: WHO.

Books

46. Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
47. Piaget, J. (1950). *The Psychology of Intelligence*. London: Routledge.
48. Ratanlal&Dhirajlal. (2016). *The Law of Torts* (27th ed.). Gurgaon: LexisNexis.
49. Turkle, S. (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books.

Journal Articles

50. Chaudhary, K. (2022). AI in Indian Classrooms: Promises and Perils. *Journal of Educational Technology & Society*, 14(3), 78–92.

51. Crootof, R. (2019). Tortious AI. *California Law Review*, 109(4), 1137–1205.
52. Guszcza, J. (2021). The Last Mile of AI Liability. *Stanford Technology Law Review*, 33, 421–478.
53. Gupta, M. (2023). Age Assurance in India: Legal and Technical Challenges. *Indian Journal of Data Protection*, 11, 45–62.
54. Hicks, M. (2023). Algorithmic Curation and Child Development. *New Media & Society*, 45(1), 112–130.
55. Jain, N., & Reddy, P. (2023). Regulating AI in India: The Missing Framework for Child Protection. *Indian Journal of Law and Technology*, 8(2), 45–72.
56. Kaminski, M. (2019). The Right to Explanation, Explained. *Berkeley Technology Law Journal*, 34, 189–248.
57. Mintz, S. (2023). COPPA at 25: Rethinking Child Online Privacy in the Age of AI. *Harvard Journal of Law & Public Policy*, 47, 1–45.
58. Sen, A. (2023). Verifiable Parental Consent under the DPDP Act. *NUJS Law Review*, 15, 301–330.

Reports and Working Papers

59. Common Sense Media. (2023). *Teens and AI: Perceptions and Vulnerabilities*. San Francisco: Common Sense Media.
60. Livingstone, S., &Stoilova, M. (2021). *The 4Cs of Online Risk: Classification Framework*. London: London School of Economics.

Websites and Online Resources

61. Global Partnership on AI. (n.d.). *Member Countries*. Retrieved from https://gpai.ai/members/
62. UNICEF. (2021). *Policy Guidance on AI for Children*. Retrieved from https://www.unicef.org/globalinsight/media/2356/file/UNICEF-Global-Insight-policy-guidance-AI-children-2021.pdf

---

Declaration by Author (s): *"We hereby declare that this manuscript is our original work, free from plagiarism, and that all sources and any use of Artificial Intelligence tools for content generation or editing have been fully disclosed and verified for accuracy."* ***Babita Pathak*** **& Dr. Santosh Kumar Tiwari**