PURC Journal of Law,
Vol. 2, Issue 1, January - June, 2026, pp. 32-50

The Watched Child: AI, Autonomy, and the Future of Privacy

Soudamini Sharma[1]

Introduction

The intensifying presence of artificial intelligence (AI) in children's everyday lives has transformed the very conditions under which childhood privacy can be understood. What once appeared as an isolated instance of digital interaction has evolved into a dense and pervasive ecosystem of AI-mediated experiences: smart toys that continuously listen, educational platforms that generate intricate learning profiles, and recommendation systems that track viewing habits with remarkable precision. These technologies do far more than collect information. They analyse, classify, and predict, gradually shaping digital identities for children long before they can comprehend the implications of such surveillance. The volume and sensitivity of the data involved, from behavioural traces and biometric indicators to subtle emotional cues, suggest that traditional privacy boundaries are being redrawn in ways existing regulatory frameworks struggle to address.[2]

This shift raises a deeper structural concern: whether privacy remains a meaningful right for children in environments expressly designed to observe, infer, and respond to them at all times. Contemporary legal protections continue to rely heavily on consent, transparency, and the assumption that children or their guardians can meaningfully evaluate risks. Yet many AI systems operate with significant opacity, learning from children's interactions without explicit notice, explanation, or avenues for contestation. In educational settings, especially,

[1] Gujarat National Law University, Gandhinagar, Gujrat, India. Soudamini25mcbl21@gnlu.ac.in
[2] Children's Privacy in the Age of Artificial Intelligence (CSA Grp., Toronto, 2021).

predictive algorithms can infer aptitude, behavioural tendencies, or perceived risk levels from patterns that are invisible to both students and caregivers.[3] These inferences can subtly influence learning pathways or institutional decisions, resulting in long-term consequences that often remain largely unexamined. Combined with children's developmental vulnerabilities, this asymmetry of power heightens the risk of misclassification and entrenches the permanence of data-driven judgments.

The broader policy landscape reflects similar tensions. Although international child-rights instruments affirm privacy as a foundational entitlement, the speed and scale at which AI reshapes childhood experiences far outpace the evolution of regulatory safeguards.[4] Many contemporary privacy regimes remain grounded in data-protection models suited to discrete acts of collection rather than continuous, inference-generating technologies. Even where child-specific principles exist, they are inconsistently implemented and often fail to address the deeper design choices that shape children's interactions with AI, choices related to developmental sensitivity, oversight, and the prioritisation of children's best interests.

These pressures make it increasingly clear that the conversation about children's privacy cannot remain confined to procedural data-protection requirements. AI now shapes how children are perceived, governed, and guided within digital spaces, subtly influencing their autonomy, cognitive development, and future opportunities. A digital footprint formed in childhood can follow an individual into adulthood, informing profiling practices by private platforms or even predictive assessments in welfare or justice systems. [5] Protecting children in such environments requires a shift away from consent-based models toward substantive, anticipatory safeguards grounded in accountability, transparency, and a nuanced understanding of children's developmental needs.

This paper positions these challenges within the broader project of safeguarding children's rights in AI-saturated environments. By examining how AI systems recalibrate privacy norms, it argues for regulatory approaches that move beyond transactional notions of data exchange and toward a rights-based framework that recognises privacy as a foundational condition for dignity, agency, and equitable futures. Children growing up in technologically mediated environments need protections that are not only reactive but participatory and

[3] "AI, Education, and Children's Rights" 10 Frontiers in Education (2025).
[4] *Ibid.*
[5] V. Charisi, et al., Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy (Joint Research Centre, European Commission, Luxembourg, 2022).

forward-looking, protections designed to ensure that childhood remains a space of growth, exploration, and possibility rather than one constrained by algorithmic judgement.

Research Questions

1. How does artificial intelligence reshape the meaning and boundaries of children's privacy in digital environments?
2. What are the major privacy risks faced by children through AI systems operating in homes, schools, and public institutions?
3. Why are existing legal and regulatory frameworks inadequate in addressing AI-driven privacy harms affecting children?
4. How do profiling, behavioural prediction, and algorithmic inference impact children's autonomy, development, and future opportunities?
5. What rights-based and child-centric safeguards can be developed to strengthen privacy protection for children in AI-mediated environments?

Research Objectives

1. To analyse how artificial intelligence reshapes the meaning and boundaries of children's privacy primarily through datafication, inference, profiling, and surveillance.
2. To identify the main environments in which children interact with AI and the risks arising in each.
3. To identify the developmental, ethical, and structural vulnerabilities that make children susceptible to algorithmic misinterpretation, bias, and long-term digital consequences.
4. To formulate rights-based, child-centric recommendations that strengthen privacy protections across diverse AI-mediated environments.

Hypothesis

The study proceeds on the hypothesis that current legal, ethical, and technological frameworks are insufficient to safeguard children's privacy in AI-mediated environments, primarily because they rely on mechanisms such as notice, consent, and generalised privacy norms that do not account for children's developmental capacities or the inferential and opaque nature of modern AI systems. It is therefore expected that a structural, rights-oriented approach is required to ensure meaningful privacy protections for children in digitally saturated contexts.

Research Methodology

This study adopts a qualitative, doctrinal, and analytical research methodology to examine the relationship among artificial intelligence, privacy, and children's rights. The research primarily relies on doctrinal analysis of legal instruments, policy documents, judicial decisions, and existing literature relating to AI governance and child protection. It also draws on secondary sources, including scholarly books, journal articles, law reviews, and expert commentaries, to understand the evolving legal and ethical concerns surrounding AI technologies.

The study further employs thematic synthesis to identify recurring issues across technology, ethics, psychology, and governance, along with a case-based analysis of AI use in homes, schools, and public institutions. Finally, a normative evaluation is undertaken to identify gaps in existing safeguards and propose rights-based recommendations for strengthening the protection of children in the age of artificial intelligence.

Scope and Limitations

Scope:

The study focuses on AI systems that collect, infer, or act upon children's data across domestic, educational, online, and institutional environments. It addresses privacy as both a legal right and a developmental need.

Limitations:

1. The study does not include empirical fieldwork with children.
2. It does not analyse jurisdiction-specific statutory compliance in detail.
3. Rapid technological evolution may render certain observations less relevant in the long term.

Significance of the Study

This research is significant because it addresses an urgent and under-examined challenge: the transformation of childhood privacy by AI systems that operate through continuous monitoring and opaque inference. The study provides:

1. A clearer conceptual understanding of privacy in AI-mediated childhoods.

2. Insight into why traditional safeguards fail in these environments;

3. A framework for developing child-centred, rights-oriented protections;

4. A contribution to ongoing debates on ethical and regulatory AI governance.

By centring children's needs, capacities, and vulnerabilities, the study advances a more responsible and future-proof approach to AI design and policy.

Conceptual Foundations

A rigorous analysis of children's privacy in the age of artificial intelligence requires two complementary conceptual anchors. First, we must understand what contemporary AI systems do, technically and epistemically, and how that activity differs from older forms of digital processing. Second, we must reconceive privacy in terms that reflect children's developmental needs and the distinctive harms they face when their lives are translated into algorithmic representations. Only by pairing a technical grasp with a rights-sensitive normative account can policy responses avoid superficial fixes that fail to address the deeper problem: AI does not merely leak or store information about children; it reshapes the conditions in which childhood itself unfolds.

Understanding Artificial Intelligence

Artificial intelligence, insofar as it is relevant to childhood privacy, should be treated as an inference-generating apparatus rather than a neutral repository. Modern AI systems, especially those driven by machine learning and deep learning, automatically detect correlations in large datasets and use those patterns to make judgments about future behaviour, preferences, or states of mind. The jump from observable action to inferred trait is the defining feature that differentiates AI from earlier technologies; it produces new, often sensitive knowledge about the child that did not exist prior to algorithmic processing.[6]

Opacity compounds risk. The internal logic of many AI systems is difficult to interpret; the weights and transformations inside a trained model rarely translate into simple, explainable

[6] UNICEF, How Can Generative AI Better Serve Children's Rights? (UNICEF Office of Global Insight, 2024), available at: https://www.unicef.org/innocenti/how-can-generative-ai-better-serve-childrens-rights (last visited on Nov. 20, 2025).

rules. Moreover, AI systems are frequently interconnected: a profile generated in one context (for instance, an adaptive learning environment) can inform recommendations or decisions in another (such as targeted content delivery), thus amplifying the reach and permanence of algorithmic judgments. The practical consequence is that children are not only observed; they are durably described and managed by systems whose architecture resists straightforward scrutiny and accountability.[7]

Finally, AI's tendency to create self-reinforcing feedback loops is a significant concern. When an algorithm designates a learner as "struggling" or a viewer as "vulnerable," the system's subsequent behaviours, recommendations, remedy prompts, or attention allocation may cement that classification. Over time, such feedback can narrow a child's opportunities and shape identity formation in ways that remain invisible, absent deliberate auditing and governance.

The Privacy Rights of Children

Privacy for children should be framed less as a transactional mechanism for data exchange and more as a developmental safeguard that protects the space for growth, experimentation, and error. Childhood involves a sequence of learning processes, social, emotional, and cognitive, that presuppose some degree of sanctuary from permanent evaluation. Privacy allows children to try, fail, and revise without the fear that a transient misstep will be translated into an enduring data profile that shapes their schooling, social opportunities, or institutional interventions. In AI-embedded environments, however, such a sanctuary is increasingly rare: continuous monitoring transforms ephemeral behaviour into persistent records subject to inference and reuse.[8]

Consent-based protections, a staple of many privacy regimes, are particularly weak when applied to children. The premise of meaningful consent presupposes an understanding of what data entail, how inferences are produced, and what downstream consequences might follow capacities that children generally lack and that caregivers frequently do not possess at the requisite technical depth. Consequently, consent risk becomes performative: checkboxes or parental authorisations often replace for basic understanding or genuine choice. This

[7] Stacey Steinberg, "The Myth of Children's Online Privacy Protection" *77 SMU Law Review 441* (2024).
[8] Anthony Owen and Dario Lam, Protecting Children's Data Privacy in AI-Enabled Early Education: Ethical Imperatives and Policy Options (2025), available at: https://www.researchgate.net/publication/395325189_Protecting_Children's_Data_Privacy_in_AI-Enabled_Early_Education_Ethical_Imperatives_and_Policy_Options (last visited on Aug. 2025).

suggests the need for alternative mechanisms that do not rely primarily on consent but instead impose limits on collection, promote data minimalism, require age-appropriate design, and embed strong avenues for redress and oversight.[9]

Moreover, privacy is inherently relational and systemic in nature. Algorithmic classifications do not affect individuals in isolation; they interact with institutional practices, such as school admissions, welfare assessments, or content moderation, producing cumulative impacts.[10]

AI in Children's Lives: Key Domains of Interaction

Artificial intelligence has woven itself into the routines of children's lives with surprising speed, often in ways that are subtle enough to escape scrutiny. What distinguishes this era is not simply that children use digital tools, but that these tools increasingly interpret, predict, and respond to them. AI systems generate behavioural inferences, shape online experiences, and influence how institutions perceive children. Understanding these points of interaction is crucial to appreciating why privacy risks arise and how they accumulate across contexts.

AI in the Home

The home traditionally a private and protective space has become a significant site of AI-mediated interaction. Smart speakers, connected toys, and home-monitoring devices routinely capture children's voices, queries, and behavioural cues. Many of these systems operate continuously, blurring the boundaries between deliberate input and ambient collection. Children may treat conversational devices as companions, unaware that their interactions generate data-rich profiles. The risk is not limited to data capture: AI-generated responses may be inaccurate, unsafe, or developmentally insensitive, revealing gaps in how such systems interpret children's language and needs.[11] What appears as harmless play may, in reality, form part of a persistent behavioural archive that neither children nor their caregivers can meaningfully oversee.

---

[9] *Ibid.*
[10] *Supra* note 6.
[11] Nomisha Kurian, "'No, Alexa, No!' Designing Child-Safe AI and Protecting Children from the Risks of the 'Empathy Gap' in Large Language Models" *50 Learning, Media and Technology 621* (2025). 11., Rachel Achieng, "AI & Children: Privacy, Trust, and Safety in the Digital Age", The Friendly Troll Podcast, Dec. 29, 2025, available at: https://cipit.org/ai-children-privacy-trust-and-safety-in-the-digital-age/ (last visited on Nov. 29, 2025).

AI in Education and Public Institutions

Schools represent another major point of contact. AI-driven learning platforms, assessment tools, and behaviour-monitoring systems promise personalised instruction and early intervention. Yet these systems often rely on extensive tracking performance trends, learning behaviours, emotional signals to produce predictions about academic potential or behavioural risk. Such classifications can follow children across school years, shaping expectations and narrowing opportunities. Children cannot opt out, and educators may not fully understand the assumptions embedded in algorithmic recommendations.

Beyond schools, public institutions increasingly adopt biometric or predictive tools, whether for identification, service delivery, or security. These systems raise accuracy concerns, particularly where algorithms perform unevenly across age groups or demographic categories.[12] Misclassification in these contexts can carry serious consequences, from reduced access to services to unwarranted institutional attention.

Across both home and institutional settings, AI normalises forms of surveillance that children may come to accept as ordinary. The cumulative effect is a shrinking of private space in which children can grow, experiment, and err without algorithmic observation. These everyday interactions form the backdrop against which privacy must be reassessed.

Nature of Privacy Risks in AI Systems

The privacy risks that AI poses to children arise not only from the volume of data collected, but from the ways AI systems *process, infer, and operationalise* that data. Unlike earlier technologies that relied on explicit inputs, AI continuously generates new interpretations of a child's behaviour, preferences, vulnerabilities, and learning patterns. These layers of inference, often invisible to users, transform ordinary digital interactions into long-term, algorithmically constructed identities. Understanding these risks requires examining how data collection, inference, and governance intersect to reshape children's privacy landscapes.

[12] Rachel Achieng, "AI & Children: Privacy, Trust, and Safety in the Digital Age", The Friendly Troll Podcast, Dec. 29, 2025, available at: https://cipit.org/ai-children-privacy-trust-and-safety-in-the-digital-age/ (last visited on Nov. 29, 2025).

Datafication and Inference

AI systems rarely limit themselves to the information children intentionally provide. They detect patterns in keystrokes, voice tones, online activity, attention levels, and even emotional cues, using these signals to predict behaviour or classify traits. This "datafication" process turns everyday actions into markers of ability, interest, or risk.[13] For children, whose behaviours fluctuate with development, such inferences risk being inaccurate yet persistent. Once encoded into algorithmic profiles, they can affect educational recommendations, content exposure, and institutional perceptions in ways neither the child nor caregivers can contest.

Profiling and Behavioural Shaping

One of the less visible risks is AI's potential to shape children's choices. Recommendation systems encourage certain viewing patterns, while adaptive platforms steer learning trajectories based on earlier performance. Although these tools appear personalised, they may limit exploration by reinforcing narrow behavioural loops. Over time, subtle steering can influence interests, habits, and self-perception effects that are particularly consequential during formative stages of identity development.

Institutional and Structural Risks

Privacy risks are also institutional. Schools, welfare agencies, and public bodies may rely on AI-generated scores, risk indicators, or biometric matches without fully understanding their limitations. Errors or biases in these systems disproportionately affect children who depend on such institutions for services or protection.[14] Furthermore, AI-driven decisions often lack transparency: children rarely know when they have been classified, what data fed the decision, or whether the classification can be challenged.

Governance Gaps

Finally, governance gaps exacerbate all other risks. Existing privacy frameworks, largely built around consent and notice, are ill-suited for technologies that operate through

[13] UNICEF Research Collaboration, "Artificial Intelligence and Children's Rights: Executive Summary" (UNICEF Research Collaboration, 2018).
[14] R. Mik, et al., "AI, Children, and the Law: Addressing Cognitive and Rights-Based Vulnerabilities" 18 *Journal of Responsible Technology* (2025), available at: https://www.sciencedirect.com/science/article/abs/pii/S2212473X2500077X (last visited on Nov. 26, 2025).

continuous inference and hidden processing. Children cannot meaningfully consent to complex data ecosystems, and adults cannot reasonably monitor the full scope of data flows.[15] Without structural safeguards, the burden of privacy protection falls on those least capable of asserting it.

Legal and Policy Landscape

The legal and policy landscape governing children's privacy in AI-mediated environments remains fragmented and uneven, reflecting a tension between rapidly evolving technologies and regulatory frameworks that largely predate them. While many jurisdictions have articulated children's rights in general terms, the translation of those principles into AI-specific safeguards is still incomplete. As a result, children are often protected by laws that were never designed to address algorithmic inferences, predictive profiling, or the continuous data flows that characterise modern AI systems.

International Standards

At the international level, child-rights instruments recognise privacy as a core entitlement grounded in dignity, identity, and autonomy. These frameworks emphasise the need for protections that reflect children's developmental vulnerabilities, the evolving nature of their capacities, and the unique harms that arise from long-term data collection.[16] Growing attention has been directed toward the digital environment, with recommendations stressing that children require default protections, transparency, and safety by design. However, these principles often lack binding force, leaving implementation to domestic systems that vary widely in ambition and scope.

Domestic Legal Approaches

Domestic laws reflect divergent philosophies. Some jurisdictions adopt protective, child-centric approaches that emphasise data minimisation, higher consent thresholds, and restrictions on profiling. Others rely heavily on general privacy laws that apply equally to adults and children, despite clear differences in comprehension, vulnerability, and power. In many places, the primary legal responses continue to revolve around notice, consent, and data retention rules frameworks that struggle to address AI's predictive capabilities or the

[15] *Supra* note 11.
[16] *Supra* note 6

structural opacity of machine-learning systems. Children, by virtue of their age, are poorly positioned to understand complex data practices, and adults often lack the expertise needed to evaluate algorithmic risks on their behalf.

Regulatory Gaps and Challenges

Regulatory gaps persist across several dimensions: limited transparency obligations for AI systems interacting with children; weak standards governing data inference; inconsistent limits on biometric processing; and minimal requirements for audits, impact assessments, or child-specific risk evaluations. Moreover, enforcement mechanisms often lag behind technical developments, meaning that even when protective laws exist, they may not adequately constrain ongoing practices.

Overall, the current legal landscape illustrates a clear mismatch: children inhabit AI-generated environments that shape their digital identities, while the laws designed to protect them remain anchored in pre-AI assumptions. Bridging this gap requires not only updating existing frameworks but also adopting approaches that recognise the structural and developmental dimensions of children's exposure to AI.

Comparative Overview of Emerging AI Regulations Across various Jurisdictions

Recent global AI regulations increasingly acknowledge children as a vulnerable group requiring specialised safeguards. The EU Artificial Intelligence Act expressly prohibits AI systems that exploit vulnerabilities arising from age, thereby banning manipulative or behaviour-shaping AI practices that may adversely affect minors.[17] Under this regime, children receive heightened protection against AI systems designed to influence their decision-making capacities or exploit developmental limitations.[18] Further, the Digital Services Act (DSA) and related EU initiatives propose a "digital minimum age" of sixteen for

[17] The Artificial Intelligence Act, 2024 (European Union), art. 5, available at: https://artificialintelligenceact.eu/article/5/ (last visited on Nov. 21, 2025).
[18] European Parliament, "New EU Measures Needed to Make Online Services Safer for Minors" (Press Release, 2025), available at: https://www.europarl.europa.eu/news/hu/press-room/20251013IPR30892 (last visited on Nov. 25, 2025).

accessing social-media and AI-enabled platforms without parental consent, reflecting a shift toward stronger online safety guarantees for minors.[19]

China has also adopted child-centric regulatory measures within its broader AI and cyberspace governance model. Its Regulations on Protecting Minors in Cyberspace require AI-driven digital service providers, schools, and guardians to implement measures that prevent harmful content exposure and improper data practices concerning children.[20]

International bodies similarly stress the necessity of embedding children's rights into AI governance. UNICEF emphasises that generative AI poses unique risks such as discrimination, lack of digital literacy, and unequal access requiring states and private actors to prioritise fairness, safety, and inclusivity for children.[21]

Despite these developments, important gaps remain. Scholars note that existing frameworks still struggle to address AI-driven deepfakes involving children, evolving challenges of age-verification, and cognitive vulnerabilities in technologically mediated environments.[22] These limitations highlight the need for explicit child-centric safeguards, including safety-by-design requirements, prohibitions on manipulative design features, and mandatory risk assessments focusing on minors' rights and developmental needs.

In India, protections for children in AI-mediated environments primarily arise from the Digital Personal Data Protection Act, 2023 (DPDP Act), which prohibits tracking, behavioural monitoring, profiling, and targeted advertising directed at minors and requires verifiable parental consent for processing children's data.[23] The DPDP Rules were officially notified in 2025, operationalising these obligations for digital and AI-enabled services that process children's personal data.[24] However, India still lacks an AI-specific statute. While the Information Technology Act, 2000 provides a general cyber-law framework, it does not address AI-driven harms such as deepfakes, algorithmic manipulation, or automated content

[19] *Ibid.*
[20] People's Republic of China, Regulations on the Protection of Minors in Cyberspace, 2023, available at: https://securiti.ai/china-regulation-to-protect-minors-in-cyberspace/ (last visited on Nov. 21, 2025).
[21] *Supra* note 5.
[22] *Supra* note 13.
[23] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on Nov. 24, 2025).
[24] Press Information Bureau, "Government Notifies Rules Under the Digital Personal Data Protection Act" (PIB Release, 2025), available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014 (last visited on Nov. 23, 2025).

risks to minors.[25] Judges of the Supreme Court have recently called for urgent AI-specific legislation to combat emerging threats such as AI-enabled child abuse and synthetic media involving children.[26] Emerging research from India also highlights concerns around adolescents' exposure to unsafe generative-AI content, digital literacy gaps, and unequal access, underscoring the need for a more explicit child-centred AI governance framework.[27]

Ethical Imperatives for Safeguarding Children's Privacy

i. **Children's vulnerability**: AI does not only collect children's data, it shapes their behaviour, opportunities, and digital identities. Ethical protection must therefore address data interpretation and inference, not just collection.

ii. **Consent limits:** Children and parents cannot meaningfully understand complex AI systems. Consent alone is insufficient; structural safeguards, minimal data collection, bans on unnecessary profiling, protective defaults, are essential.

iii. **Data minimisation:** Child-facing systems often collect excessive behavioural and emotional data. Minimisation prevents such data from drifting into advertising, analytics, or institutional scoring, reducing long-term harms.

iv. **Transparency & explainability:** Children require clear, age-appropriate explanations of when AI is used, what it does, and where errors may occur. Transparency supports autonomy and digital literacy.

v. **Contestability:** When AI mislabels or misclassifies a child, simple and accessible mechanisms for correction and human review must be built into systems.

vi. **Fairness & non-discrimination:** AI tools used with children must be audited for bias, especially since marginalised groups are more likely to be misclassified. Ethical practice requires diverse datasets, continuous monitoring, and restrictions on high-risk uses.

---

[25] International Association of Privacy Professionals (IAPP), "Global AI Governance: India" (IAPP, 2024), available at: https://iapp.org/resources/article/global-ai-governance-india/ (last visited on Nov. 20, 2025).

[26] Editorial, "Supreme Court Judge Calls for Legislation on AI-Enabled Deepfakes and Child Abuse", Mathrubhumi, 2025, available at: https://english.mathrubhumi.com/news/india/justice-nagarathna-legislation-deepfakes-ai-child-abuse-cl0aalr8 (last visited on Nov. 30, 2025).

[27] Kasturi, et al., "Children, Rights and AI in India" (LSE Research Papers, 2025), available at: https://eprints.lse.ac.uk/129517/1/Rights.AI_India_Kasturi_et_al_2025.pdf (last visited on Nov. 30, 2025).

Case Studies Illustrating Core Privacy Risks

Examining concrete examples of AI deployment offers a clearer picture of how children's privacy risks manifest in practice. These case studies drawn from home environments, educational settings, and broader digital ecosystems demonstrate how seemingly benign technologies can produce significant ethical and developmental challenges for children. They highlight patterns that recur across contexts: opacity, misinterpretation, data overreach, and a tendency toward automated judgment that children cannot meaningfully contest.

AI Voice Assistants in Domestic Spaces

AI-enabled voice assistants are now common in homes, but they pose significant privacy risks for children. These systems sometimes provide harmful or developmentally inappropriate responses because they lack the ability to understand context and emotions. Beyond explicit queries, they also capture ambient sounds, background conversations, and the voices of multiple household members often without full user awareness. This turns the home into a space of continuous algorithmic monitoring. Children, who tend to anthropomorphise such devices, may share sensitive information with misplaced trust, exposing them to both immediate privacy intrusions and long-term risks of inference, profiling, and data sharing.[28]

Adaptive Learning Platforms in Schools

AI-driven educational platforms offer personalised learning, but they also generate detailed behavioural and performance profiles through continuous monitoring of keystrokes, response times, errors, and emotional cues. The risks emerge when these data-driven interpretations shape a child's academic path: early labels such as "inattentive" or "low-performing" can channel students into restrictive tracks, creating self-reinforcing cycles that limit future opportunities. Although often treated as neutral tools, these systems can embed biases from their training data, while families have little insight into how recommendations are produced. The opacity of these models makes it difficult to contest errors, increasing the influence of automated judgments over a child's educational trajectory.[29]

[28] *Supra* note 10.
[29] *Supra* note 11.

Biometric Identification and Surveillance

Biometric technologies such as facial recognition, fingerprint scanning, and gait analysis are increasingly deployed in schools and public institutions, collecting highly sensitive data that children cannot change if compromised. Accuracy remains a significant concern: facial recognition systems often perform poorly on children due to rapid physical changes and training datasets built around adult faces, leading to misidentification, exclusion, or unwarranted interventions. Continuous biometric monitoring can also cause children to internalise a sense of constant surveillance, affecting their developing expectations of privacy. Structural risks persist around data storage, retention, and sharing; weak safeguards enable "mission creep," where biometric data collected for one purpose is repurposed for others without meaningful consent or oversight.[30]

Recommendations and Safeguards for Protecting Children's Privacy

Addressing the privacy risks children face in AI-mediated environments requires more than incremental reform; it calls for a structural reorientation of how AI is designed, deployed, and governed. Effective safeguards must therefore operate at multiple levels, with an emphasis on anticipatory protections rather than reactive enforcement.[31]

Strengthening Regulatory and Policy Frameworks

Legal systems must evolve to address AI's inferential capabilities, especially its ability to generate sensitive insights about children. Regulations should set firm limits on profiling and automated decision-making that affects children's rights or future opportunities.[32] Core privacy principles, data minimisation, and purpose limitation must be enforced strictly, including prohibitions on repurposing children's data for commercial targeting or institutional risk scoring. Given children's heightened vulnerabilities, the law should require safety-by-design measures, child-specific data-retention limits, and mandatory impact assessments that evaluate risks related to bias, developmental harm, and discrimination.

[30] *Supra* note 4.
[31] *Ibid.*
[32] *Supra* note 5.

Technical Safeguards and Child-Centric Design

Technical protections are essential at the design stage. AI systems used with children should incorporate privacy-by-design and security-by-design features that minimise data collection, enable rapid deletion of behavioural data, and ensure strong encryption.[33] Child-centred design also requires explainability: systems must provide age-appropriate cues indicating when AI is operating and offer clear pathways for seeking help. High-risk tools such as biometrics, emotional analytics, or predictive profiling should be heavily restricted or banned in children's settings unless justified by a compelling and narrowly defined need.[34]

Institutional Accountability and Human Oversight

Schools and public institutions must not deploy AI tools without clear governance structures. Policies should specify who reviews algorithmic outputs, who corrects errors, and how decisions influenced by AI are documented. No child should be subjected to automated decisions without meaningful human oversight capable of interpreting context and intervening. Training for educators and frontline workers is critical to ensure they understand AI's limits and the developmental implications of relying on algorithmic assessments.[35]

Transparency and Rights of Redress

Children and families need accessible, age-appropriate information about how AI systems operate, what data they collect, how it is used, and with whom it is shared. Transparency must be paired with strong redress mechanisms: the ability to challenge errors, request corrections or deletion, and obtain explanations for automated classifications.[36] Oversight bodies, whether independent commissions or designated regulators, should have the authority to investigate complaints, mandate audits, and impose penalties for misuse of children's data.

Conclusion

This study aimed to investigate how artificial intelligence (AI) reshapes the privacy landscape of children's lives and to test the hypothesis that existing legal and ethical frameworks are insufficient to address the distinctive risks posed by AI. The analysis across the preceding

[33] *Supra* note 7.
[34] *Supra* note 4.
[35] *Supra* note 6.
[36] *Supra* note 2.

sections confirms this hypothesis convincingly. At every stage, whether in the home, in schools, or in public institutions, children encounter AI systems that interpret, predict, and respond to them in ways that exceed the scope of traditional privacy protections. These systems do not merely collect information; they generate new forms of knowledge about children, often with little transparency and even less oversight. As a result, children are placed within environments that constantly observe and classify them, thereby narrowing the protective space essential for healthy development.

By mapping the domains in which children routinely engage with AI, it became evident that privacy risks are neither abstract nor episodic. They accumulate through everyday interactions with smart toys that listen indefinitely, with school platforms that profile academic tendencies, and with biometric tools that freeze a child into a fixed category despite the fluidity of childhood. These encounters reveal ethical and developmental vulnerabilities that general privacy frameworks often overlook. Children cannot meaningfully consent, cannot recognise when they are being profiled, and cannot contest algorithmic judgments that may shape their opportunities.

The study offers a framework rooted in structural and anticipatory safeguards. These include embedding privacy and safety by design into all child-facing AI systems, limiting data collection to what is genuinely necessary, ensuring age-appropriate explainability, strengthening human oversight, and developing rights-based regulatory approaches capable of scrutinising algorithmic profiling. The analysis also recognises the importance of including children's own perspectives, an element often overlooked in policymaking, but essential for designing systems that reflect their needs and expectations. By foregrounding children's insights and aligning them with ethical and policy considerations, the study advances not only a theoretical model but a practical roadmap for reform.

Taken together, the research confirms that protecting children's privacy in the age of AI is not simply a matter of updating existing laws or improving technical procedures. It requires rethinking the conditions under which children grow, learn, and interact with digital systems. The conclusion emerging from this study is both clear and urgent: meaningful protection of children's privacy demands a shift from individual responsibility to structural accountability. Only through a coordinated effort spanning legal reform, ethical design, institutional responsibility, and participatory engagement can we ensure that AI evolves in ways that honour children's dignity, autonomy, and developmental freedoms. In this sense, the study

not only validates its hypothesis but also articulates a vision of governance that is responsive to the realities of digital childhoods and capable of safeguarding them for the future.

Bibliography

Books

- Noble, Safiya Umoja, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press, 2018).
- Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

Statutes, Treaties & International Instruments

- Convention on the Rights of the Child (UN Office of the High Commissioner for Human Rights).
- General comment No. 25 (2021) Children's rights in relation to the digital environment (UN Committee on the Rights of the Child).
- Regulation (EU) 2016/679 , General Data Protection Regulation.
- Digital Personal Data Protection Act, 2023 (India)
- Proposal for a Regulation on artificial intelligence (EU Artificial Intelligence Act)

Journals, Articles & Research Papers

- Charisi, Vasiliki et al., *Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy* (Joint Research Centre, European Commission , Science for Policy report, 2022).
- CIPIT (Centre for IP & IT Law), Rachel Achieng, "AI & Children: Privacy, Trust, and Safety in the Digital Age" (2023).
- CSA Group, *Children's Privacy in the Age of Artificial Intelligence* (CSA Group research report, 2021).

- Kurian, Nomisha, "'No, Alexa, No!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models," *Learning, Media and Technology* (2024)
- Owen, Anthony & Dario Lam, *Protecting Children's Data Privacy in AI-Enabled Early Education: Ethical Imperatives and Policy Options* 2025
- Steinberg, Stacey B., "The Myth of Children's Online Privacy Protection," *SMU Law Review* (2024)
- UNICEF, *Policy Guidance on AI for Children* (UNICEF Innocenti policy guidance global insight, 2021)