International Journal of Computer Applications Technology and Research
Volume 13–Issue 12, 214 – 225, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1312.1017

Protecting Children’s Data Privacy Rights in the Artificial Intelligence Era: A Legal and Human Rights Approach

Olamide Olatomike Ajala
University of Dayton
School of Law
USA

Abstract: The rapid integration of artificial intelligence (AI) into digital platforms has fundamentally transformed how children’s personal data are collected, processed, and exploited. From educational technologies and social media to healthcare applications and smart devices, children are increasingly subjected to data-driven profiling, automated decision-making, and behavioral prediction at an unprecedented scale. This development raises profound legal and human rights concerns, as children constitute a uniquely vulnerable group with limited capacity to understand, consent to, or challenge complex data practices embedded in opaque AI systems. This article adopts a legal and human rights-based approach to examine the adequacy of existing frameworks for protecting children’s data privacy in the AI era. It situates children’s data protection within international human rights law, emphasizing the rights to privacy, dignity, autonomy, and the best interests of the child. The analysis then narrows to AI-specific risks, including algorithmic opacity, persistent digital identities, surveillance, and discriminatory outcomes. By critically evaluating data protection regimes, AI governance instruments, and enforcement mechanisms, the article identifies regulatory gaps and accountability challenges. It argues for child-centered AI governance that embeds privacy, transparency, and accountability by design, ensuring that technological innovation progresses without undermining children’s fundamental rights in the digital age.

Keywords: Children’s data privacy, Artificial intelligence governance, Human rights law, Data protection regulation, Algorithmic accountability, Child-centered digital rights

1. INTRODUCTION

1.1 The Digitalization of Childhood and Rise of AI Systems

The digitalization of childhood has expanded steadily as children engage with educational technologies, online games, health applications, and social media platforms as part of everyday life [1]. Digital learning environments generate continuous records of attendance, assessment performance, interaction patterns, and behavioral indicators, embedding data collection into routine educational processes [2]. Gaming platforms capture preferences, reaction times, communication styles, and in-game transactions, while social platforms record social networks, images, location signals, and expressive behaviors [3]. Health and wellbeing technologies further contribute to this data ecosystem by collecting sensitive information related to physical activity, sleep, and biometric signals, often through connected or wearable devices [4].

Artificial intelligence systems increasingly govern how these diverse data streams are processed and interpreted. Machine learning techniques enable automated profiling, predictive modeling, and behavioral inference that shape content recommendations, advertising exposure, educational tracking, and risk classification [5]. Unlike traditional data processing, AI systems generate secondary inferences that extend beyond the original purpose of collection, producing enduring digital identities that may influence future opportunities [6].

Children represent a uniquely vulnerable group of data subjects within this environment due to developmental immaturity, limited legal capacity, and pronounced information asymmetries [7]. They often lack the ability to understand complex data practices or anticipate long-term consequences, while parental consent mechanisms struggle to address opaque and continuously learning systems [8]. These vulnerabilities are compounded by commercial incentives and cross-platform data sharing, increasing exposure to surveillance, manipulation, and discriminatory outcomes [9].

1.2 Framing Children’s Data Privacy as a Legal and Human Rights Issue

Framing children’s data privacy as a legal and human rights issue shifts attention from narrow regulatory compliance toward the protection of fundamental interests essential to human dignity and development [1]. Privacy in this context is not merely a procedural requirement satisfied through disclosure notices or consent mechanisms, but a substantive right that safeguards autonomy, identity formation, and freedom from undue interference [4]. For children, whose personal and social identities are still evolving, data-driven intrusions may generate cumulative and irreversible effects across education, employment, and civic participation [7].

This approach draws on the intersection of data protection law, child protection law, and international human rights norms. Data protection regimes articulate principles such as lawfulness, fairness, purpose limitation, and data minimization, while explicitly recognizing children as deserving enhanced safeguards [2]. Child protection frameworks emphasize vulnerability, best interests, and protection from exploitation, extending established welfare principles into digital environments shaped by algorithmic decision-making [6]. Human rights law provides the overarching normative foundation by embedding children’s data privacy within rights to private life, equality, development, and participation [3].

Adopting a human rights lens also clarifies the positive obligations of states to regulate private actors whose technologies shape children’s lived experiences [8]. It requires assessing proportionality, necessity, and accountability when permitting AI-driven data practices, rather than deferring to innovation narratives alone [5]. This normative framing establishes the conceptual basis for evaluating AI risks, regulatory adequacy, and governance mechanisms discussed in subsequent sections, ensuring that technological progress remains compatible with children's fundamental rights [9].

2. NORMATIVE AND HUMAN RIGHTS FOUNDATIONS OF CHILDREN'S DATA PRIVACY

2.1 The Right to Privacy and Data Protection in International Human Rights Law

The right to privacy is firmly established within international human rights law as a core safeguard of human dignity, autonomy, and personal development [7]. Foundational human rights instruments recognise privacy as protection against arbitrary or unlawful interference with an individual's private life, family, home, and correspondence, creating obligations for states to respect and protect this right [8]. Initially conceived in relation to physical spaces and interpersonal communications, privacy has progressively expanded to encompass informational dimensions as societies have become increasingly data-driven [9].

This evolution marked a shift from a narrow conception of privacy toward a broader framework of data protection. Data protection principles emerged to address systematic collection, storage, and processing of personal information by public and private actors, emphasizing fairness, lawfulness, purpose limitation, and accountability [10]. Unlike traditional privacy rights, data protection focuses not only on secrecy but also on governance of information flows, risk mitigation, and individual control over personal data.

As digital technologies advanced, these principles were increasingly applied to automated and large-scale processing environments. In AI-mediated contexts, personal data is no longer merely recorded but continuously analyzed, combined, and repurposed to generate predictions and inferences [11]. International human rights law remains applicable in these environments, requiring states to ensure that emerging technologies do not undermine established protections [12]. The use of algorithmic systems does not displace privacy obligations but intensifies the need for safeguards, particularly where opaque processing and long-term data retention amplify risks. This human rights grounding provides the normative baseline for assessing how children's data should be protected within increasingly complex digital and AI-driven systems [13].

2.2 Children's Rights Principles Relevant to Data Privacy

Children's data privacy must be interpreted through core principles of children's rights law, which recognize children as rights holders requiring enhanced and tailored protection [14]. Central among these principles is the best interests of the child, which requires that all decisions affecting children prioritize their overall wellbeing, development, and long-term interests. In data-driven environments, this principle demands scrutiny of whether data practices genuinely serve children's needs or primarily advance commercial or institutional objectives [9].

The concept of evolving capacities further shapes children's data protection. As children mature, their ability to understand, participate in, and influence decisions affecting them increases, requiring graduated approaches to consent, information provision, and participation [10]. Data governance frameworks must therefore accommodate children's growing autonomy while still providing safeguards appropriate to their developmental stage. Participation rights also imply that children should, where appropriate, have a voice in how technologies that affect them are designed and governed [11].

Children's rights law additionally emphasizes special protection against exploitation and harm. Digital environments create new vectors for economic exploitation, manipulation, and profiling, particularly where data is monetized or used to influence behavior [12]. Data privacy protections function as preventive mechanisms that reduce exposure to such harms by limiting excessive data collection and inference. Integrating these principles ensures that children's data protection is not treated as an abstract technical issue, but as an essential component of safeguarding childhood development, dignity, and equality in technologically mediated societies [8].

2.3 Children as a Distinct Class of Data Subjects

Children constitute a distinct class of data subjects due to developmental, structural, and relational factors that differentiate their position from that of adults in digital environments [7]. Cognitive development affects children's ability to understand complex data processing practices, foresee long-term consequences, and exercise informed consent. Even where consent mechanisms exist, they often rely on legal proxies or simplified disclosures that fail to capture the implications of AI-driven inference and profiling [13].

Power asymmetries further intensify these vulnerabilities. Technology platforms possess significant informational, economic, and technical power, while parents and guardians may lack the expertise or leverage needed to challenge opaque systems [11]. States, meanwhile, may struggle to regulate transnational data flows and rapidly evolving technologies effectively [9]. These imbalances limit meaningful choice and accountability for children affected by data-driven decisions.

Recognizing children as a distinct category of data subjects justifies heightened legal safeguards and contextual risk assessment. It also provides the analytical bridge toward AI-specific concerns, where automated decision-making, persistent profiling, and predictive analytics pose amplified risks to children's rights, autonomy, and future opportunities [14].

3. ARTIFICIAL INTELLIGENCE AND EMERGING RISKS TO CHILDREN'S DATA PRIVACY

3.1 Data Collection, Profiling, and Automated Decision-Making Involving Children

Artificial intelligence systems increasingly shape how children's data are collected, aggregated, and operationalized across digital environments [13]. In educational settings, algorithmic systems analyze attendance records, learning behaviors, assessment scores, and engagement metrics to personalize content, predict academic performance, and flag perceived risks [14]. Advertising and content recommendation systems similarly rely on behavioral data drawn from gaming platforms, social media interactions, and browsing patterns to infer preferences, vulnerabilities, and consumption tendencies [15]. These practices extend beyond surface-level personalization, embedding children within complex profiling infrastructures that continuously adapt and learn.

A defining feature of AI-driven processing is the creation of persistent digital identities. Data collected during childhood is often retained, recombined, and repurposed over long periods, enabling the construction of longitudinal profiles that may influence future educational opportunities, commercial targeting, or institutional assessments [16]. Unlike transient observations, algorithmic inferences can harden into reputational signals that follow children across platforms and life stages, frequently without transparency or avenues for correction. The early formation of such profiles raises concerns about path dependency, where past data constrains future possibilities.

These dynamics introduce significant risks of discrimination, manipulation, and exclusion. Algorithmic systems trained on biased or incomplete data may disproportionately disadvantage certain groups of children, reinforcing social inequalities along lines of socioeconomic status, ethnicity, disability, or geography [17]. Behavioral targeting techniques may exploit developmental vulnerabilities, shaping choices and preferences in ways that undermine autonomy [18]. Automated decision-making can also exclude children from opportunities or services without meaningful explanation or recourse.

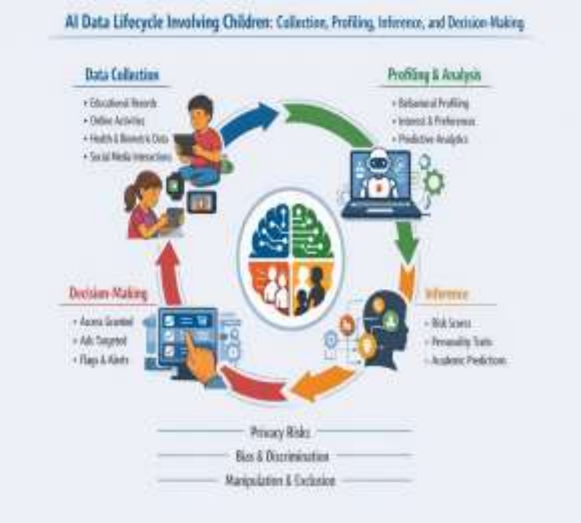

Figure 1: *AI Data Lifecycle Involving Children: Collection, Profiling, Inference, and Decision-Making*

Together, these practices transform children from passive data subjects into continuously evaluated data objects. The scale, persistence, and opacity of AI-driven profiling distinguish these risks from earlier forms of data processing, necessitating focused legal and human rights scrutiny [19].

3.2 Opacity, Explainability, and Children's Rights

A central challenge posed by AI systems affecting children is opacity. Many machine learning models operate as "black boxes," producing outputs that are difficult to interpret even for experts [20]. For children and their guardians, understanding how decisions are made becomes nearly impossible, particularly when systems rely on complex data correlations rather than explicit rules. This lack of transparency undermines the ability to contest decisions that affect educational placement, content exposure, or risk classification.

Explainability is especially significant in contexts involving children's rights. Effective explanation requires not only technical transparency but also communication adapted to children's cognitive and developmental capacities [14]. Information provided to parents or guardians may be overly technical, incomplete, or disconnected from children's lived experiences. As a result, procedural safeguards such as notice and consent often fail to deliver meaningful understanding or control [17].

From a legal perspective, opacity raises concerns about accountability and due process. Where automated decisions have significant effects on children, the inability to explain underlying logic limits oversight, regulatory enforcement, and access to remedies [15]. Explainability functions as a prerequisite for challenging discriminatory or disproportionate outcomes and for assessing compliance with legal principles such as fairness and proportionality.

In human rights terms, opaque AI systems risk transforming children into subjects of unaccountable power. Without visibility into how decisions are made, children's rights to participation, dignity, and development are weakened [18]. Ensuring explainability is therefore not merely a technical aspiration but a legal requirement tied to transparency, accountability, and effective protection of children's data privacy [13].

3.3 Surveillance, Behavioral Prediction, and Autonomy Erosion

AI-driven data practices increasingly enable pervasive surveillance of children's behaviors across digital and physical spaces. In educational contexts, monitoring technologies track attendance, attention, emotional states, and disciplinary indicators, often justified by efficiency or safety objectives [16]. These systems normalize continuous observation, reshaping learning environments into spaces of constant evaluation.

Beyond monitoring, predictive behavioral analytics seek to anticipate future conduct, academic outcomes, or social risks. Such systems may classify children as "high-risk" or "low-performing" based on historical data and inferred traits [19]. While framed as preventive or supportive, predictive models can stigmatize children and limit opportunities through self-fulfilling classifications. Emerging practices resembling social scoring amplify these concerns by aggregating diverse data points into composite evaluations of behavior or character [14].

These forms of surveillance and prediction erode children's autonomy. Awareness of constant monitoring may suppress experimentation, self-expression, and dissent, which are critical to healthy development [20]. Moreover, predictive systems can shape expectations imposed by institutions, narrowing the range of choices available to children before they can exercise agency. When surveillance becomes embedded within everyday environments, opting out is rarely feasible. The cumulative effect is a shift from supportive oversight to anticipatory control, raising profound concerns for children's rights to privacy, freedom, and identity formation [17].

3.4 From Technological Risk to Legal Responsibility

The risks associated with AI-driven data practices affecting children cannot be addressed solely through technical safeguards or ethical guidelines. Surveillance, profiling, opacity, and predictive decision-making translate into concrete harms that engage legal responsibility [18]. Framing these issues as technological challenges alone obscures the role of law in setting limits, allocating accountability, and providing remedies.

International human rights and data protection frameworks impose duties on states to protect children from rights-infringing practices by private actors [13]. This includes regulating AI systems, enforcing transparency and proportionality, and ensuring access to effective redress. By shifting the focus from innovation-driven risk acceptance to rights-based governance, legal systems can transform technological risks into enforceable obligations. This transition provides the foundation for evaluating regulatory frameworks and accountability mechanisms in subsequent sections [20].

4. LEGAL FRAMEWORKS GOVERNING CHILDREN'S DATA IN THE AI ERA

4.1 Data Protection Law and Enhanced Protections for Children

Modern data protection law recognizes children as deserving enhanced protection due to their vulnerability and limited capacity to fully understand data-processing practices [18]. Core principles such as lawfulness, fairness, transparency, purpose limitation, and data minimization apply with heightened force where children's personal data are involved. Legislators and regulators increasingly emphasize that data practices affecting children must be designed with their best interests in mind, rather than relying on generic compliance mechanisms suitable for adults [19].

Special protections for children's data often include stricter conditions for lawful processing. Certain categories of data such as biometric, health, or behavioral data are treated as particularly sensitive when linked to children, requiring additional safeguards and justifications [20]. These protections reflect the recognition that misuse or overexposure of such data can have long-term developmental and social consequences.

Consent thresholds and parental authorization mechanisms represent a central feature of children's data protection regimes. Laws typically impose age-based thresholds below which parental or guardian consent is required for lawful processing [21]. However, consent alone is not considered sufficient where processing is excessive, opaque, or unnecessary. Regulators increasingly stress that reliance on parental consent does not absolve data controllers from assessing proportionality, necessity, and risk.

Lawful processing is further constrained by purpose limitation requirements, which restrict the use of children's data to clearly defined and legitimate objectives [22]. AI-driven repurposing of data for secondary uses, such as profiling or commercial targeting, challenges this principle by blurring original and subsequent purposes. As a result, data protection law provides an essential but incomplete foundation for regulating AI systems involving children, necessitating complementary AI-specific rules [23].

4.2 Children's Data in AI-Specific Regulatory Frameworks

AI-specific regulatory frameworks increasingly adopt a risk-based approach that classifies systems according to their potential impact on fundamental rights, including the rights of children [24]. Under this model, AI applications involving children particularly in education, health, or behavioral monitoring are more likely to be categorized as high risk due to their influence on development and life opportunities [18]. This classification triggers enhanced obligations related to risk assessment, transparency, human oversight, and accountability.

Risk-based regulation acknowledges that not all AI systems pose equal threats. Systems that merely automate administrative tasks are treated differently from those that profile, predict, or make decisions about children's abilities, behavior, or future prospects [19]. For high-risk systems, regulators increasingly require pre-deployment impact assessments that explicitly evaluate effects on children's rights and wellbeing.

Some frameworks go further by prohibiting certain AI practices involving children altogether. These include forms of manipulative behavioral targeting, indiscriminate biometric surveillance, or social scoring mechanisms that rank children based on aggregated behavioral data [20]. Where outright prohibitions are not imposed, strict safeguards are mandated to ensure human oversight, explainability, and avenues for contestation.

Table 1: Comparative Overview of Children's Data Protections Across Major Data and AI Laws

Legal / Regulatory Instrument	**Primary Scope**	**Child Definition / Age Threshold**	**Core Children-Specific Data Protections**	**AI / Automated Decision-Making Controls Relevant to Children**	**Enforcement / Remedies**
EU GDPR	General personal data processing (public + private sectors)	"Child" not uniformly defined; **parental consen**	"Children merit specific protection"; **heightened transparency**, fairness; stricter expectations	Restrictions on **solely automated decisions** with legal/similarly significant effects; rights to	Data protection authorities; administrative fines; data

Legal / Regulatory Instrument	**Primary Scope**	**Child Definition / Age Threshold**	**Core Children-Specific Data Protections**	**AI / Automated Decision-Making Controls Relevant to Children**	**Enforcement / Remedies**
		t required for information society services below a **Member State-set age (13–16)**	around lawful basis and **data minimization** for children; stronger stance against exploitative marketing	information and safeguards; **profiling** scrutiny where impacts are significant	subject rights (access, erasure, objection), complaints, judicial remedies
UK GDPR + Data Protection Act 2018 (and Age-Appropriate Design Code)	UK version of GDPR + children's online design expectations	Similar to GDPR; consent age generally aligned with **13** for online services	Age-appropriate design expectations: **high privacy by default**, data minimization, limits on nudge/engagement patterns; stronger expectations for transparency suited to children	Strong emphasis on **risk-based design** and accountability for profiling/recommendation systems affecting children	ICO regulatory oversight; audits, enforcement notices, fines; complaints and judicial routes
United States COPPA	Online services directed to children; collection of data from children	**Under 13**	**Verifiable parental consent** before collection/use/disclosure; clear notice; limits on data retention; reasonable security; restrictions on marketing/data-sharing practices	Indirect—controls apply to data feeding AI models; AI profiling risk governed mainly through data collection limits and consent	FTC enforcement; consent decrees; penalties; compliance programs
United States FERPA	Student education records held by educational agencies/institutions receiving federal funds	Students in covered institutions; parents hold rights until student becomes "eligible student" (typically 18 or postsecondary)	Controls **disclosure** of education records; consent requirements for release; rights of access and correction	Indirect—limits use/sharing of student records that can fuel predictive analytics; does not comprehensively regulate vendor AI inference	U.S. Dept. of Education enforcement; loss of funding (rare); complaint processes
United States HIPAA	Protected health information held by covered entities (healthcare providers/insurers) and business associates	Minors included; parental access varies by state and context	Strict rules for **use/disclosure**, security safeguards; minimum necessary; special rules for certain sensitive services (state-dependent)	Indirect—limits on how pediatric health data can be used in AI systems by covered entities; does not comprehensively govern consumer health apps outside scope	HHS OCR enforcement; civil penalties; corrective action plans; breach notification duties
EU AI Act (risk-based AI regulation)	AI systems placed on the market/used in covered contexts	Not defined by age; protects fundamental rights broadly (children treated	Focuses on **risk controls** for AI systems likely to affect children (e.g., education, biometrics, safety-	**High-risk AI obligations** (risk management, data governance, documentation, transparency, human oversight);	Market surveillance authorities; conformity assessment requirements;

Legal / Regulatory Instrument	Primary Scope	Child Definition / Age Threshold	Core Children-Specific Data Protections	AI / Automated Decision-Making Controls Relevant to Children	Enforcement / Remedies
		as higher-risk group in impact contexts)	related uses)	restrictions/prohibitions for certain practices; relevance to child-facing profiling and monitoring	penalties for noncompliance
Council of Europe / human-rights oriented instruments (privacy + child rights principles)	Human rights standards guiding privacy and child protection	Child generally understood as **under 18**	Best interests, dignity, protection from exploitation; reinforces state duties to protect children from harmful digital practices	Sets normative expectations: legality, necessity, proportionality, accountability—useful for assessing opaque AI profiling and surveillance	Enforced via domestic incorporation, courts, and oversight bodies (varies by state)

AI-specific regulation thus complements data protection law by addressing risks arising from automation, inference, and scale. However, effective protection depends on consistent interpretation and enforcement, particularly where children's data is processed across borders and sectors [21]. The interaction between data protection and AI governance remains a critical area for legal development [22].

4.3 Sector-Specific Legal Protections

Beyond general data protection and AI regulation, sector-specific legal frameworks play a crucial role in safeguarding children's data. In education technology, laws and policies increasingly regulate how student data is collected, used, and shared by schools and private vendors [23]. These rules often restrict commercial exploitation of educational data and require that processing align with pedagogical purposes rather than advertising or profiling objectives.

Digital health and biometric systems involving children are subject to heightened scrutiny due to the sensitivity and permanence of health-related data [24]. Legal safeguards typically require explicit authorization, strict security measures, and limitations on secondary use. The integration of AI into pediatric diagnostics or wellbeing monitoring raises additional concerns about accuracy, bias, and accountability, reinforcing the need for sector-tailored oversight [18].

Online platforms and social media represent another critical domain. Laws governing children's online services increasingly mandate age-appropriate design, limits on targeted advertising, and default privacy protections [19]. These measures aim to counteract business models that incentivize excessive data collection and behavioral engagement.

While sector-specific regimes provide targeted safeguards, fragmentation remains a challenge. Children often interact with multiple sectors simultaneously, leading to overlapping or inconsistent protections [20]. This fragmentation underscores the need for coordinated governance mechanisms that align sectoral rules with overarching human rights and data protection principles [21].

4.4 Gaps, Fragmentation, and Jurisdictional Challenges

Despite the expansion of legal protections, significant gaps and challenges persist. Cross-border data flows complicate enforcement, as children's data is frequently processed in jurisdictions with differing legal standards [22]. Multinational technology companies may exploit regulatory inconsistencies, limiting the effectiveness of national protections.

Enforcement capacity also varies widely. Regulatory authorities often face resource constraints, technical complexity, and limited powers to audit AI systems affecting children [23]. These challenges are exacerbated by the opacity of algorithmic processing and the difficulty of demonstrating harm before it materializes.

Fragmentation across legal regimes further weakens protection. Data protection, AI regulation, consumer law, and child protection frameworks may operate in parallel without sufficient coordination [24]. As a result, children's data privacy can fall through regulatory gaps. Addressing these challenges requires a shift toward integrated governance and accountability models that recognize children's data protection as a cross-cutting legal priority. This transition sets the stage for examining enforcement, corporate responsibility, and rights-based governance mechanisms in the following section [18].

5. ACCOUNTABILITY, GOVERNANCE, AND ENFORCEMENT MECHANISMS

5.1 State Obligations and Regulatory Oversight

States bear primary responsibility for safeguarding children's rights in digital environments, including protection against privacy infringements arising from private-sector use of artificial intelligence [21]. Under international human rights law, this duty extends beyond non-interference to include positive obligations to regulate, monitor, and enforce standards governing data practices that affect children. Where AI systems are deployed by commercial actors in education, health, or online services, states must ensure that legal frameworks effectively prevent foreseeable harm and provide meaningful safeguards [22].

Regulatory oversight is central to fulfilling these obligations. Data protection authorities play a critical role in supervising compliance with data protection principles, investigating complaints, and imposing sanctions where children's data is processed unlawfully or excessively [23]. Their mandate increasingly intersects with that of child protection agencies, which possess expertise in assessing vulnerability, best interests, and developmental impacts. Effective oversight therefore requires coordination between regulatory bodies to address both technical data risks and broader child welfare concerns.

However, regulatory challenges persist. AI systems are often complex, adaptive, and opaque, limiting the ability of authorities to audit decision-making processes or identify discriminatory effects [24]. Resource constraints and jurisdictional limitations further undermine enforcement capacity, particularly where platforms operate across borders. To address these challenges, states are increasingly encouraged to adopt proactive oversight tools, including mandatory risk assessments, algorithmic audits, and reporting obligations for high-risk systems involving children. Such measures strengthen accountability by shifting regulatory intervention upstream, before harm occurs, and by reinforcing the state's role as guarantor of children's fundamental rights in AI-mediated environments [25].

5.2 Corporate Responsibility and Due Diligence

Alongside state obligations, corporate actors bear independent responsibility to respect children's rights when developing and deploying AI systems [26]. Human rights-based data governance frameworks emphasize that companies should not rely solely on legal compliance, but actively identify, prevent, and mitigate adverse impacts on children arising from their data practices. This responsibility is particularly acute for technology firms whose business models depend on large-scale data collection, profiling, and behavioral prediction.

Due diligence processes provide a structured mechanism for operationalizing corporate responsibility. Children's rights impact assessments enable organizations to evaluate how AI systems may affect children's privacy, autonomy, and wellbeing across the data lifecycle [21]. These assessments encourage early identification of risks related to excessive data collection, discriminatory outcomes, or manipulative design features. Importantly, effective due diligence requires meaningful engagement with stakeholders, including child rights experts, educators, and, where appropriate, children themselves.

Embedding children's rights into corporate governance also involves design choices. Privacy-by-design and safety-by-design approaches require that data minimization, transparency, and age-appropriate protections are integrated into AI systems from the outset, rather than added retrospectively [23].

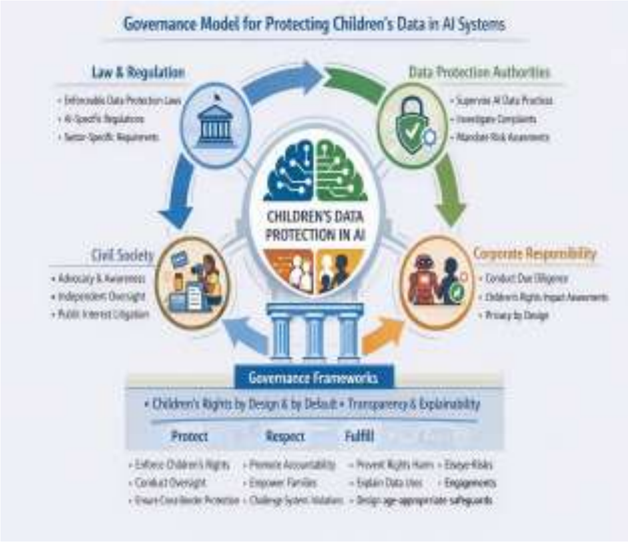
Governance Model for Protecting Children's Data in AI Systems
Law & Regulation
• Enforceable Data Protection Laws
• AI-Specific Regulations
• Sector-Specific Requirements
Data Protection Authorities
• Supervise AI Data Practices
• Investigate Complaints
• Mandate Risk Assessments
CHILDREN'S DATA PROTECTION IN AI
Civil Society
• Advocacy & Awareness
• Independent Oversight
• Public Interest Litigation
Corporate Responsibility
• Conduct Due Diligence
• Children's Rights Impact Assessments
• Privacy by Design
Governance Frameworks
• Children's Rights by Design & by Default • Transparency & Explainability
Protect
Respect
Fulfill
• Enforce Children's Rights
• Conduct Oversight
• Ensure Cross-Border Protection
• Promote Accountability
• Empower Families
• Challenge System Violations
• Prevent Rights Harm
• Explain Data Uses
• Design age-appropriate safeguards
• Ensure Risks
• Engagements

Figure 2: *Governance Model for Protecting Children's Data in AI Systems*

Through robust governance structures, companies can align innovation with rights-respecting practices, reducing legal risk while contributing to the protection of children's data in increasingly automated environments [27].

5.3 Remedies, Redress, and Access to Justice for Children

Effective protection of children's data privacy requires accessible remedies and avenues for redress when rights are violated [22]. Complaint mechanisms administered by data protection authorities offer a primary route for addressing unlawful data processing, yet procedural complexity and limited awareness can hinder children's access to these processes. Ensuring child-friendly procedures and representation is therefore essential.

Beyond individual complaints, collective redress mechanisms and public interest litigation play an important role in addressing systemic harms arising from AI-driven data practices [24]. Such approaches enable civil society organizations and regulators to challenge widespread violations that may not be apparent through isolated cases. They are particularly relevant where harms are diffuse, long-term, or difficult to attribute to specific decisions.

Access to justice also encompasses the availability of corrective measures, including data erasure, cessation of unlawful processing, and compensation where appropriate [26]. However, remedies must be forward-looking as well as corrective. Preventive measures, transparency obligations, and ongoing monitoring help ensure that violations do not recur. Strengthening remedial frameworks thus supports a transition from reactive enforcement to anticipatory governance, laying the groundwork for future-oriented safeguards that better protect children's rights in evolving AI ecosystems [27].

6. BALANCING INNOVATION, AI DEVELOPMENT, AND CHILDREN'S RIGHTS

6.1 The Tension Between Technological Innovation and Child Protection

Artificial intelligence innovation is frequently justified through narratives of efficiency, personalization, and societal progress, particularly in education, health, and digital services used by children [24]. These narratives often frame regulatory intervention as a barrier to technological advancement, suggesting that stringent legal constraints may hinder experimentation and economic growth. However, when applied to children's data, innovation-led reasoning risks subordinating fundamental rights to market imperatives. Children's exposure to AI-driven profiling and predictive analytics illustrates how innovation can generate irreversible consequences when safeguards are insufficient [25].

A rights-based perspective challenges the assumption that innovation and protection are inherently incompatible. Legal limitations on data collection, inference, and automation do not prohibit innovation, but rather define acceptable boundaries within which innovation must occur. Where AI systems influence children's educational trajectories, behavioral assessment, or access to opportunities, the absence of constraints may entrench inequality and systemic bias [26].

Concerns about regulatory chilling effects are often overstated. Carefully designed regulation can promote responsible innovation by clarifying expectations, reducing legal uncertainty, and incentivizing trust-enhancing design choices. For children, regulatory restraint serves not as a deterrent to progress but as a mechanism for ensuring that technological development aligns with long-term social interests [27]. Balancing innovation and protection therefore requires shifting from permissive experimentation toward precautionary governance that prioritizes children's rights without foreclosing beneficial technological applications.

6.2 Embedding Children's Rights by Design and by Default

Embedding children's rights by design and by default represents a proactive strategy for reconciling AI development with legal and human rights obligations [28]. Privacy-by-design principles require that data minimization, purpose limitation, and security safeguards are integrated into AI systems from their inception rather than retrofitted after deployment. When applied to children's data, these principles demand heightened sensitivity to developmental vulnerability and long-term impact.

Safety-by-design extends this approach by addressing risks beyond data misuse, including manipulation, discrimination, and autonomy erosion. Child-centric AI design models prioritize age-appropriate interfaces, transparent decision logic, and limitations on profiling and behavioral prediction [24]. Such models recognize that children's interaction with technology differs fundamentally from that of adults and must be reflected in system architecture.

Operationalizing rights by default also requires organizational commitment. Developers and deployers must treat children's rights considerations as core design parameters rather than compliance checklists. This approach shifts responsibility upstream, reducing reliance on consent mechanisms that often fail to provide meaningful protection [29]. By embedding legal and ethical constraints into technical systems, rights-based design transforms child protection from a reactive response into a structural feature of AI innovation.

7. FUTURE DIRECTIONS: TOWARD CHILD-CENTERED AI GOVERNANCE

7.1 Emerging Policy and Regulatory Trends

Policy approaches to children's data protection increasingly emphasize anticipatory governance, which seeks to address risks before harm materializes [30]. Rather than responding solely to violations after deployment, regulators are exploring forward-looking tools such as mandatory impact assessments, pre-market conformity checks, and ongoing monitoring of high-risk AI systems involving children.

A parallel trend is gradual global convergence around shared principles, even in the absence of uniform binding law. Soft-law instruments, guidelines, and international cooperation frameworks contribute to harmonizing expectations regarding transparency, accountability, and child-specific safeguards [25]. While these instruments lack direct enforceability, they influence regulatory interpretation and corporate behavior, shaping emerging norms.

Anticipatory governance also reflects recognition that children's data protection must evolve alongside technology. Static rules struggle to address adaptive AI systems, making flexible, principle-based approaches increasingly important [27]. These trends signal a shift toward governance models that treat children's rights as foundational constraints on AI development rather than afterthoughts.

7.2 Ethical, Educational, and Societal Dimensions

Legal safeguards alone are insufficient to protect children's data privacy in AI-driven environments. Ethical, educational, and societal measures play a complementary role in shaping responsible data practices [28]. Digital literacy initiatives aimed at children and parents enhance understanding of data flows, profiling risks, and automated decision-making, enabling more informed engagement with technology.

Schools occupy a pivotal position in this ecosystem. As primary adopters of educational technologies, they influence procurement decisions, data governance standards, and everyday data practices [24]. Integrating data protection awareness into curricula also empowers children to recognize and question intrusive technologies. Civil society organizations further contribute by advocating for children's rights, conducting independent oversight, and supporting strategic litigation where systemic harms arise [29].

Ethical discourse reinforces the notion that children should not bear disproportionate risks in the pursuit of innovation. Societal engagement helps translate abstract rights into shared expectations about acceptable uses of AI.

Table 2: Key Policy Tools for Strengthening Children's Data Privacy in AI Systems

Policy Tool	Primary Objective	Key Features	Relevance to AI Systems Involving Children	Contribution to Children's Rights Protection
Children's Rights Impact Assessments (CRIA)	Identify and mitigate risks to children's rights before deployment	Systematic evaluation of privacy, autonomy, discrimination, and developmental impact; stakeholder consultation	Applied to AI systems used in education, health, online platforms, and behavioral analytics	Ensures **best interests of the child** are considered ex ante; prevents foreseeable harm
Privacy-by-Design and Safety-by-Design Requirements	Embed protection into system architecture	Data minimization, purpose limitation, secure defaults, age-appropriate interfaces	Reduces excessive data collection, profiling, and opaque inference in child-facing AI	Translates legal principles into technical safeguards; protects dignity and autonomy
Risk-Based AI Classification Frameworks	Allocate regulatory obligations proportionate to potential harm	Categorization of AI systems as low, medium, or high risk; enhanced duties for high-risk uses	Flags AI systems influencing children's education, behavior, or opportunities as high risk	Strengthens preventive regulation and accountability for impactful systems
Explainability and Transparency Standards	Enable understanding and contestation of automated decisions	Clear information on logic, purpose, and consequences of AI decisions; age-appropriate communication	Critical where AI affects educational placement, content curation, or profiling of children	Supports participation rights, due process, and effective remedies
Limits and Prohibitions on Certain AI Practices	Prevent inherently harmful or exploitative uses	Restrictions on manipulative behavioral targeting, indiscriminate biometric surveillance, or social scoring	Addresses AI practices that pose disproportionate risks to children's development	Establishes clear red lines consistent with human rights protection
Enhanced Regulatory Oversight and Auditing Powers	Ensure compliance and ongoing accountability	Algorithmic audits, reporting obligations, enforcement powers for regulators	Enables supervision of opaque or adaptive AI systems affecting children	Strengthens state duty to protect children from private-sector abuses
Child-Friendly Complaint and Redress Mechanisms	Improve access to justice for children	Simplified procedures, representation, collective complaints, public interest litigation	Addresses diffuse or long-term harms caused by AI-driven data practices	Ensures remedies are accessible, effective, and rights-respecting
Digital Literacy and Public Awareness Programs	Empower children, parents, and educators	Education on data rights, AI risks, and privacy-protective practices	Complements legal safeguards by improving informed engagement with AI systems	Reinforces autonomy, participation, and societal accountability
International Cooperation and Soft-Law Instruments	Address cross-border data and AI governance gaps	Shared standards, guidelines, regulatory cooperation	Relevant where children's data flows across jurisdictions	Promotes consistency and global protection of children's rights

8. AN INTEGRATED LEGAL AND HUMAN RIGHTS FRAMEWORK FOR CHILDREN'S DATA PROTECTION

8.1 Synthesizing Legal, Technological, and Human Rights Approaches

An integrated framework for children's data protection in AI systems must align legal norms, technological design, and human rights principles within a coherent governance architecture [30]. Data protection law provides enforceable standards, AI regulation addresses automation-specific risks, and human rights law supplies the normative foundation that prioritizes dignity, development, and equality. Integration ensures that protections do not operate in isolation or conflict.

Such a framework emphasizes lifecycle governance, addressing risks from data collection through inference and decision-making. It also recognizes children as distinct rights holders requiring contextual safeguards. By embedding rights across regulatory, technical, and institutional layers, integration enhances consistency, accountability, and effectiveness [26].

8.2 Implications for Policymakers, Regulators, and Technology Developers

For policymakers and regulators, an integrated approach requires coordination across legal domains and proactive oversight of AI systems affecting children [27]. Fragmented regulation must be replaced with shared standards and enforcement mechanisms that reflect the cross-sectoral nature of children's data use.

For technology developers, integration translates into operational responsibility. Rights-based governance demands that legal and ethical constraints inform design decisions, business models, and deployment strategies from the outset [29].

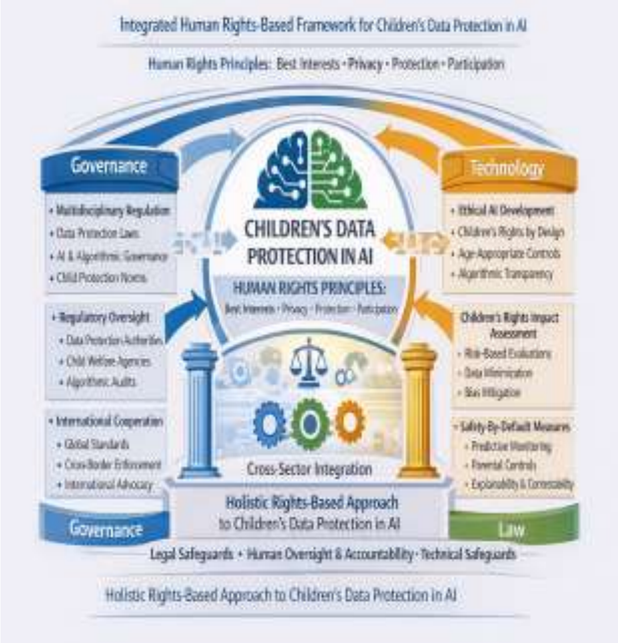
Integrated Human Rights-Based Framework for Children's Data Protection in AI
Human Rights Principles: Best Interests • Privacy • Protection • Participation
Governance
• Multidisciplinary Regulation
• Data Protection Laws
• AI & Algorithmic Governance
• Child Protection Norms
• Regulatory Oversight
• Data Protection Authorities
• Child Welfare Agencies
• Algorithmic Audits
• International Cooperation
• Global Standards
• Cross-Border Enforcement
• International Advocacy
CHILDREN'S DATA PROTECTION IN AI
HUMAN RIGHTS PRINCIPLES:
Best Interests • Privacy • Protection • Participation
Cross-Sector Integration
Technology
• Ethical AI Development
• Children's Rights by Design
• Age-Appropriate Controls
• Algorithmic Transparency
Children's Rights Impact Assessment
• Risk-Based Evaluations
• Data Minimization
• Bias Mitigation
• Safety-By-Default Measures
• Predictive Monitoring
• Parental Controls
• Explainability & Contestability
Governance
Holistic Rights-Based Approach to Children's Data Protection in AI
Law
Legal Safeguards • Human Oversight & Accountability • Technical Safeguards
Holistic Rights-Based Approach to Children's Data Protection in AI

Figure 3: *Integrated Human Rights-Based Framework for Children's Data Protection in AI*

Together, these implications underscore that protecting children's data privacy is not an obstacle to innovation but a prerequisite for sustainable, rights-respecting AI development [30].

9. CONCLUSION: SAFEGUARDING CHILDREN'S PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE

9.1 Key Legal and Human Rights Insights

This article has reaffirmed that children's data privacy is not a peripheral regulatory concern but a fundamental legal and human rights issue that lies at the heart of dignity, autonomy, and healthy development. As artificial intelligence systems increasingly mediate children's access to education, healthcare, social interaction, and information, data practices have become deeply embedded in the conditions under which childhood is experienced. The analysis demonstrates that traditional notions of privacy, focused narrowly on secrecy or consent, are insufficient to address the scale, persistence, and inferential power of AI-driven data processing.

A legal and human rights approach clarifies that children are entitled to enhanced protection due to their developmental vulnerability, limited agency, and the long-term consequences of early data exposure. International human rights norms, data protection principles, and child-specific legal frameworks converge in recognizing children as distinct rights holders whose interests must be prioritized over commercial or administrative convenience. Importantly, the risks posed by AI profiling, surveillance, discrimination, and opacity are not speculative but structurally embedded within many contemporary digital systems.

The core insight is that children's data privacy must be understood as a precondition for the enjoyment of other rights, including education, equality, participation, and freedom of thought. Protecting children's data is therefore not simply about preventing misuse, but about preserving the conditions for open development, self-determination, and social inclusion in increasingly automated societies.

9.2 Pathways for Sustainable and Rights-Respecting AI Futures

Looking forward, sustainable and rights-respecting AI futures depend on embedding children's rights at the center of technological governance. This requires moving beyond reactive enforcement toward proactive, anticipatory frameworks that address risks before harm occurs. Long-term governance strategies must integrate legal regulation, institutional oversight, and technical design, ensuring that accountability is distributed across states, corporations, and developers rather than shifted onto children or parents.

Effective protection also demands continuity over time. Children's data governance cannot be episodic or sector-specific; it must account for the cumulative nature of data collection and the enduring impact of early digital profiling. Rights-respecting AI futures therefore rely on lifecycle-based approaches that regulate data from initial collection through inference, decision-making, and retention. Transparency, explainability, and meaningful avenues for contestation must be treated as core system features rather than optional safeguards.

Equally important is the social dimension of governance. Education, digital literacy, and public engagement are essential to building shared understanding of acceptable uses of AI involving children. Schools, families, civil society, and policymakers all play complementary roles in shaping norms and expectations. Ultimately, sustainable AI innovation is not achieved by minimizing regulation, but by aligning technological development with the fundamental rights and long-term wellbeing of children, ensuring that progress today does not compromise the freedoms and opportunities of future generations.

10. REFERENCE

1. Rayhan R, Rayhan S. AI and human rights: Balancing innovation and privacy in the digital age. Comput. Sci. Eng. 2023;2:353964.
2. Faisal K. Certain Legal Aspects of Children's Right to Protect Personal Data in the Context of AI under the European Union Data Protection Laws. teoksessa Päivi Korpisaari (toim.), Vapaita sanoja. Viestintäoikeuden vuosikirja. 2022:109.
3. Shehu VP, Shehu V. Human rights in the technology era–Protection of data rights. European Journal of Economics. 2023 Jun;7(2).
4. Feyikemi Mary Akinyelure. Bridging the gap: Integrating predictive analytics with culturally competent mental health care delivery in marginalized populations. Int J Res Psychiatry 2023;3(2):12-17. DOI: 10.22271/27891623.2023.v3.i2a.76
5. Gilani SR, Al-Matrooshi AM, Khan MH. Right of privacy and the growing scope of artificial intelligence. Current Trends in Law and Society. 2023 Sep 19;3(1):1-1.
6. Walters R, Novak M. Cyber security, artificial intelligence, data protection & the law. Berlin: Springer; 2021 Aug 24.
7. Babikian J. Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. Law Research Journal. 2023 Dec 31;1(2):91-101.
8. Ishii K. Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. AI & society. 2019 Sep 1;34(3):509-33.
9. La Fors K. Legal Remedies For a Forgiving Society: Children's rights, data protection rights and the value of forgiveness in AI-mediated risk profiling of children by Dutch authorities. Computer Law & Security Review. 2020 Sep 1;38:105430.
10. Feyikemi Mary Akinyelure. AI in mental health diagnostics: Ethical imperatives and design strategies for equitable implementation. Int. J. Res. Med. Sci. 2021;3(2):14-19. DOI: 10.33545/26648733.2021.v3.i2a.167
11. Baruwa A. Redefining global logistics leadership: integrating predictive AI models to strengthen U.S. competitiveness. *International Journal of Computer Applications Technology and Research*. 2019;8(12):532–547. doi:10.7753/IJCATR0812.1010
12. Holmes W, Persson J, Chounta IA, Wasson B, Dimitrova V. Artificial intelligence and education: A critical view through the lens of human rights, democracy and the rule of law. Council of Europe; 2022 Nov 30.
13. Hoxhaj O, Halilaj B, Harizi A. Ethical implications and human rights violations in the age of artificial intelligence. Balkan Social Science Review. 2023 Dec 25;22(22):153-71.
14. Ebepu OO, Okpeseyi SBA, John-Ogbe JJ, Aniebonam EE. Harnessing data-driven strategies for sustained United States business growth: a comparative analysis of market leaders. *Journal of Novel Research and Innovative Development (JNRID)*. 2024 Dec;2(12):a487. ISSN: 2984-8687.
15. Bogani R, Schafer B. Artificial intelligence and children’s rights. Psychology. 2022;2213:2230.
16. Wachter S, Mittelstadt B. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Colum. Bus. L. Rev.. 2019:494.
17. Manheim K, Kaplan L. Artificial intelligence: Risks to privacy and democracy. Yale JL & Tech.. 2019;21:106.
18. Završnik A. Criminal justice, artificial intelligence systems, and human rights. InERA forum 2020 Mar (Vol. 20, No. 4, pp. 567-583). Berlin/Heidelberg: Springer Berlin Heidelberg.
19. Aderinmola RA. Scaling climate capital: market instruments and demand-side policies to mobilize institutional investment for U.S. renewable infrastructure. *International Journal of Computer Applications Technology and Research*. 2024 Dec;13(12). doi:10.7753/IJCATR1312.1012.
20. Katyal SK. Private accountability in the age of artificial intelligence. UCLA L. Rev.. 2019;66:54.
21. Medvedeva M, Vols M, Wieling M. Using machine learning to predict decisions of the European Court of Human Rights. Artificial Intelligence and Law. 2020 Jun;28(2):237-66.
22. Baruwa A. AI powered infrastructure efficiency: enhancing U.S. transportation networks for a sustainable future. *International Journal of Engineering Technology Research & Management*. 2023 Dec;7(12). ISSN: 2456-9348.
23. Yuste R, Genser J, Herrmann S. It’s time for neuro-rights. Horizons. 2021 Jan 1;18:154-64.
24. Ishay MR. The human rights reader: Major political essays, speeches, and documents from ancient times to the present. Routledge; 2022 Nov 1.
25. Cath C. Governing artificial intelligence: ethical, legal and technical opportunities and challenges. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2018 Nov 28;376(2133):20180080.
26. Nemitz P. Constitutional democracy and technology in the age of artificial intelligence. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2018 Nov 28;376(2133):20180089.
27. Nguyen A, Ngo HN, Hong Y, Dang B, Nguyen BP. Ethical principles for artificial intelligence in education. Education and information technologies. 2023 Apr;28(4):4221-41.
28. Huang C, Zhang Z, Mao B, Yao X. An overview of artificial intelligence ethics. IEEE Transactions on Artificial Intelligence. 2022 Jul 28;4(4):799-819.

29. Farhud DD, Zokaei S. Ethical issues of artificial intelligence in medicine and healthcare. Iranian journal of public health. 2021 Nov;50(11):i.
30. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC medical ethics. 2021 Sep 15;22(1):122.