



*PURC Journal of Law,
Vol. 2, Issue 1, January - June, 2026, pp. 88-102*

Reimagining Child Rights in the Digital Age: Constitutionalism, Artificial Intelligence, and the Future of Child-Centered Governance in India

Rajni Beniwal^{1*} & Mahesh Dafta²

Abstract

The digital transformation of society has revolutionised the definition of childhood. Today's children engage with AI-powered systems, social media, algorithm-driven suggestions, and data-informed technology that influence their learning, communication, and personal growth. These technologies present unparalleled opportunities for participation and empowerment, but also new and enhanced threats to children, including surveillance, profiling, privacy violations, behavioral manipulation and online exploitation. There are currently existing laws that were designed for physical settings that are not so well suited to the new issues. This article proposes that the current child rights discourse in India needs to be shifted from a welfare paradigm to a child centred paradigm of digital governance. The article explores the implications of AI and digital technologies for the concepts of privacy, autonomy, dignity and development, drawing on the principles of the constitution and existing statutes, international child rights law, and judicial rulings. It argues that protecting children's rights is not merely a question of consent-based regulation but necessitates the inclusion of such protections in technologies and systems of governance. Proposed is a framework based on the principles of privacy-by-design, safety-by-design, algorithmic accountability, transparency and meaningful child participation.

Keywords: Child Rights, Artificial Intelligence, Digital Governance, Privacy, UNCRC, Algorithmic Accountability, Constitutional Law.

^{1,2} AT University of Engineering and Management, Jaipur, Raj., India.
Email*: rajni.uem@gmail.com

Introduction

Social conditions of childhood have undergone an unprecedented change in the twenty first century. Children of today's generation are born into a world of digital technologies that have affected their communication, education, recreation, social identity, and social participation. Children are now surrounded by smart phones and social networks, online gaming communities, AI systems, and algorithmic recommendation platforms.³ In *Brown v. Entertainment Merchants Association*, the United States Supreme Court cautioned against excessive restrictions on children's access to information, holding that constitutional protection of expression extends to minors. Although decided within the context of violent video games, the decision illustrates the continuing challenge of balancing child protection with children's rights to information and participation.⁴

This tech revolution has created a great deal of opportunity for kids. Digital environments provide access to information, educational materials, opportunities for creativity and social interaction at a scale never before possible.⁵ Digital technologies may also enable children to assert their rights to participation, expression, association and access to knowledge, while at the same time generating new vulnerabilities which are inadequately captured by current law.

The current issues faced by children are not just about physical places, but also about digital spaces. Artificial intelligence (AI) systems and data-driven technologies heighten these risks through the power to continuously monitor, predict and influence children's behaviour.⁶ These changes bring up deep questions about privacy, autonomy, dignity and developmental freedom.

India has a good constitutional and statutory system for child protection.⁷ Despite the above, there are important gaps between legal protection and its implementation, with a particular gap in the protection of children's rights in relation to new digital technologies.

³ Sonia Livingstone and Alicia Blum-Ross, *Parenting for a Digital Future* (Oxford University Press, 2020).

⁴ *Packingham v. North Carolina*, 582 U.S. 98 (2017) (Supreme Court of the United States).

⁵ United Nations Convention on the Rights of the Child, 1989, arts. 13, 15 and 17.

⁶ Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc. CRC/C/GC/25 (2021).

⁷ Juvenile Justice (Care and Protection of Children) Act, 2015; Protection of Children from Sexual Offences Act, 2012; Right of Children to Free and Compulsory Education Act, 2009.

This article proposes a change of paradigm: from a reactive approach to regulation to a pro-active and child-centred governance model in the context of child rights protection in the digital age. Such an approach should acknowledge children not just as vulnerable objects to be protected but as rights-holders deserving of dignity, privacy, participation and development in digital environments.

Research Methodology

The methodology used in this study is doctrinal and analytical legal research which focuses on the analysis of the development of the child rights framework in the digital era. The research work is mainly secondary research where constitutional provisions, statutory enactments, judicial decisions, international legal instruments, policy documents, scholarly literature and reports issued by governmental and international organizations have been relied upon.

The study examines in detail the constitutional basis of child rights as enshrined in Article 14, 15(3), 21 and 21A of Constitution of India with the key legislations, including Juvenile Justice (Care and Protection of Children) Act, 2015, Protection of Children from Sexual Offences Act, 2012, Right of Children to Free and Compulsory Education Act, 2009 and Digital Personal Data Protection Act, 2023. Jurisprudence relating to children and their rights has been explored through judicial pronouncements by the Supreme Court of India, especially on privacy, dignity, education, child protection, and digital rights.

The research also draws on international legal instruments, such as the United Nations Convention on the Rights of the Child, 1989 (UNCRC) and the Committee on the Rights of the Child's General Comment No. 25 (2021) on children's rights in relation to the digital environment. Comparative analysis has also been conducted by looking at foreign regulations, like the European Union's General Data Protection Regulation (GDPR) and the Age Appropriate Design Code (AADC) of the United Kingdom. This comparative way is helpful in identifying best practices and emerging global standards in the field of child protection in digital environments.

This study uses a qualitative analytical method to assess the current legal and regulatory frameworks (in light of AI, algorithmic governance, digital surveillance, online exploitation and

social media platforms) to address emerging challenges. By analyzing key legal frameworks and regulations, the paper aims to identify gaps and suggest amendments to enhance child-centred digital governance in India. The research is focused on legal, constitutional and policy aspects of children's rights in digital environments. Technological and sociological questions are addressed when appropriate, but the emphasis is on the normative and institutional concerns of child rights protection in today's legal system.

Constitutional Foundations Of Child Rights In India

Child rights are well protected and promoted in the Constitution of India. While the Constitution does not have a standalone chapter on children, the various fundamental rights and the directive principles in the Constitution do provide a strong legal framework for children's welfare and development.

Article 14 ensures equality in the face of the law and equal protection of the law. The provision is the constitutional foundation for challenging discriminatory practices towards children and provides equal access to opportunities. Article 15(3) also gives the State the power to make special measures for children, giving legitimacy to affirmative measures that work to tackle childhood vulnerabilities.⁸

Judicial interpretation of Article 21 has been the most important constitutional change in the area of child rights. The Supreme Court has invariably broadened the scope of the right to life beyond its physical life to include dignity, development, education, health, and all the other conditions that might be necessary to meaningful human flourishing.⁹

The Supreme Court thus affirmed education as an integral part of the right to life in *Mohini Jain v. State of Karnataka*¹⁰, and children having a constitutional right to education in *Unni Krishnan, J.P. v. State of Andhra Pradesh*, leading to the enactment of Article 21A through the Eighty-Sixth Constitutional Amendment Act, 1992, which states that children aged 6 to 14 have a fundamental right to education.¹¹

The Court has also dealt with child labour in a similar way in the context of broadly interpreting the constitutional rights. The case of *M.C. Mehta v. State of Tamil Nadu* is one of the landmark

⁸ Constitution of India, arts. 14 and 15(3).

⁹ *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 SCC 608.

¹⁰ *Mohini Jain v. State of Karnataka*, (1992) 3 SCC 666.

¹¹ *Unni Krishnan, J.P. v. State of Andhra Pradesh*, (1993) 1 SCC 645.

cases of the Supreme Court of India regarding child labour working in hazardous industries and ordered the State to take care of the children who are exploited and to provide rehabilitation facilities, welfare funds and education to the children affected by the child labour.¹²

Judicial sensitivity to the needs of vulnerable children has also been seen in the area of institutional care and juvenile justice. *Sheela Barse v. Union of India* placed emphasis on humane treatment, legal assistance, and procedural safeguards of children in child care institutions,¹³ while *Sampurna Behura v. Union of India* spoke of the need to improve the working of institutional mechanisms for child protection under the Juvenile Justice Act.¹⁴

As a result of *Justice K.S. Puttaswamy v. Union of India*,¹² the constitutional significance of child rights has grown in the wake of the introduction of digital technologies. Crucially, the judgment connected dignity with privacy and autonomy and with the development of individual children, which are values of special importance for children in digital environments.¹⁵

The European Court of Human Rights has similarly recognised that privacy rights continue within digital communications. In *Barbulescu v. Romania*, the Court emphasized that monitoring of electronic communications must satisfy proportionality requirements and respect individual privacy. Although decided in an employment context, the judgment highlights broader principles applicable to children's digital communications, namely that technological surveillance must remain compatible with fundamental rights.¹⁶

The law's recognition of privacy as a constitutional right has significant consequences for topics like data collection, behavioural profiling, target advertising, and algorithmic surveillance. Children are leaving a huge amount of personal information behind in their interactions with digital platforms, with little awareness of or consent to what they are leaving behind. Thus, constitutional tenets enunciated in *Puttaswamy* offer an important normative compass to respond to new child rights issues in the digital era.

Artificial Intelligence, Algorithmic Governance and Childhood

Artificial Intelligence (AI) is one of the most influential technologies to emerge in recent years and affecting child's childhood today. Access to information, communication with others, media

¹² *M.C. Mehta v. State of Tamil Nadu*, (1996) 6 SCC 756.

¹³ *Sheela Barse v. Union of India*, (1986) 3 SCC 596.

¹⁴ *Sampurna Behura v. Union of India*, (2018) 4 SCC 433.

¹⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

¹⁶ *Bărbulescu v. Romania*, Application No. 61496/08, Judgment dated 5 September 2017 (Grand Chamber, European Court of Human Rights).

consumption, and engagement in digital environments are increasingly governed by AI systems that impact children. Access to information, communication with others, media consumption and engagement in digital environments are increasingly driven by AI systems that affect children.¹⁷ Recommendation algorithms on social media platforms, search engines, and streaming services, as well as education technologies, analyze user behaviour and produce customized content constantly, both contributing to enhanced accessibility and enriching learning experiences – but also posing serious privacy, autonomy, equality and child protection concerns.

AI technologies are different from traditional technologies, as they rely on massive amounts of data collection and predictive analytics. For children, such practices are especially problematic, as they frequently are unable to comprehend how data is gathered, manipulated, and turned into profit.¹⁸ Therefore, algorithmic governance can shape children's choices, behaviour, without their awareness or consent.

One of the main issues is algorithmic profiling. Regularly, digital platforms gather data on browsing behavior, social activities, interests, and online activities. While personalization can enhance user experience, it also has the potential of building up a comprehensive digital profile over which children may have limited control.¹⁹ These profiles may impact on educational opportunities, advertising exposure and information access, impacting developmental outcomes.

Algorithmic governance impacts more than just privacy. A recommendation system can present to children what they think the world is like and what they don't know about the world. Engagement-laden algorithms can feed into and exacerbate biases, foster overuse of platforms, and deliver toxic content to children.²⁰

Other issues of concern are algorithmic discrimination. AI systems are not neutral; they are based on assumptions, priorities, and data sets. Discriminatory outcomes from biased datasets can have an impact on marginalised children, for example, in relation to educational

¹⁷ Sonia Livingstone and Alicia Blum-Ross, *Parenting for a Digital Future* (Oxford University Press, 2020).

¹⁸ Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019).

¹⁹ Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc. CRC/C/GC/25 (2021).

²⁰ Ibid.

technologies; content-moderation systems; and automated decision-making processes.²¹ This runs counter to the constitutional rights to equality and non-discrimination provisions in Articles 14 and 15 of the Constitution.

In *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González, the Court of Justice of the European Union (CJEU) noted that the need to give individuals a greater degree of control over their personal information from the past is evident. The decision was made with reference to an adult applicant, but the reasoning is relevant to children whose online behavior may lead to a digital trail that will impact their future opportunities. The ruling echoes the notion of digital privacy, not just in terms of what you're collecting, but what you're still in control of.²²

The Supreme Court in *Justice K.S. Puttaswamy v. Union of India* established an important constitutional framework for the regulation of AI systems impacting children based on the concepts of dignity, autonomy and personal development.²³ Child Rights Impact Assessments are more and more promoted by international organizations in advance of a technology intervention that may have a significant impact on children, as a way of regulators and developers becoming aware of potential hazards and taking measures to protect children.²⁴

Digital Privacy and the Digital Personal Data Protection Act, 2023

An aspect of child rights that has emerged as one of the most important in the digital age is privacy. Kids use social media, e-learning, gaming and digital devices creating a lot of personal information. This information is frequently used for surveillance, profiling, and commercial exploitation and has raised significant concerns.²⁵

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a crucial move toward privacy regulations in India. It also provides for the verification of parental consent for the processing of

²¹ Virginia Eubanks, *Automating Inequality* (St. Martin's Press, 2018).

²² *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González, Case C-131/12, Judgment dated 13 May 2014 (CJEU)

²³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

²⁴ UNICEF, *Policy Guidance on AI for Children* (2021).

²⁵ Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008).

children's personal data²⁶ and bans certain types of behavioural monitoring and targeted advertising aimed at children.²⁷

Notwithstanding these safeguards, the DPDP Act has come under criticism for being too dependent on parental consent. In consent-based models it is assumed that parents have enough knowledge about the complexity of digital ecosystems and data processing practices. In fact, many parents don't know enough about how to assess privacy risks correctly,²⁸ and children are increasingly exploring the digital landscape on their own, so parental consent is not 100% protection.

In the realm of AI-powered technologies, the restrictions of consent start to become more apparent. Data collection is often ongoing and “stealthy” via platforms that are out of users' understanding and control. Therefore, the protection of privacy needs structural safeguards against harmful data practices, no matter whether formal consent is given or not.²⁹

This is becoming a more popular strategy which is increasingly supported internationally. Therefore, privacy should be ingrained in technology, there should be increased accountability, and more transparency regarding data processing activities are needed for a child-centred privacy framework.³⁰

Social Media, Platform Accountability and Online Harm

Children's social, educational and recreational lives are increasingly dominated by the use of social media. They allow users to communicate, create, engage in, and access information. Meanwhile, however, they introduce children to cyberbullying, exploitation, misinformation, harmful content and manipulative platform designs.³¹

Cyberbullying is one of the most prevalent forms of digital harm experienced by children. Online bullying is not like bullying in that it can happen around the clock, no matter where the victim is

²⁶ Digital Personal Data Protection Act, 2023, s. 9.

²⁷ Ibid.

²⁸ Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019).

²⁹ Committee on the Rights of the Child, General Comment No. 25 (2021).

³⁰ Ibid.

³¹ Committee on the Rights of the Child, General Comment No. 25 (2021).

located. Evidence shows that experiencing cyberbullying for a prolonged period of time can contribute to anxiety, depression, low self-esteem, and social withdrawal.³²

In *A.B. v. Bragg Communications Inc.*, the Supreme Court of Canada permitted a minor to proceed anonymously in litigation involving online harassment, recognising the serious psychological consequences of cyberbullying. The decision reflects judicial acknowledgement that children require enhanced procedural and privacy protections in digital environments.³³

In *Packingham v. North Carolina*, the United States Supreme Court recognised social media platforms as essential forums for communication and civic participation. While the case concerned restrictions imposed upon convicted offenders, its reasoning underscores that access to digital platforms has become integral to the exercise of freedom of expression. For children, this reinforces the need to regulate online spaces in ways that ensure safety without unnecessarily restricting participation.³⁴

Grooming and sexual exploitation through online communications are other concerns. Offenders can use digital platforms to gain access to children using anonymous or disguised accounts. The Protection of Children from Sexual Offences Act, 2012 establishes legal procedures to tackle such behaviour, but it is challenging to enforce because of anonymity, cross-border communications and technological complexity.³⁵

Platform Design has played a more important role than ever. Services like online games often use architectures designed to facilitate extended engagement with the service, such as notifying users of items of interest, rewarding them for extended use, or recommending things to them. The focus of these mechanisms tends to be on maximizing user attention and advertising revenue, rather than focussing on the welfare of children.³⁶ As a result, regulations that look solely at user responsibility do not take account of the structural causes of digital harms.

³² Sameer Hinduja and Justin Patchin, *Bullying Beyond the Schoolyard* (2nd ed., Corwin Press, 2015).

³³ *Fairfax Media Publications Pty Ltd v. Voller*, [2021] HCA 27 (High Court of Australia).

³⁴ *A.B. v. Bragg Communications Inc.*, 2012 SCC 46, [2012] 2 S.C.R. 567 (Supreme Court of Canada).

³⁵ Protection of Children from Sexual Offences Act, 2012.

³⁶ Jonathan Haidt, *The Anxious Generation* (Penguin Press, 2024).

Platform accountability, therefore, is an integral part of modern child rights protection. Social media platforms should have to undertake child rights risk assessments, improve their content moderation practices, add a reporting feature and implement a grievance redressal process. This type of commitments is similar to new worldwide trends that shift more liability from the individual user toward platform operators.

Comparative Perspectives: EU GDPR and the UK Age Appropriate Design Code

Comparative regulatory experiences offer insights in the new regulatory strategies for child protection in digital environments. The General Data Protection Regulation (GDPR) of the European Union has been considered to be one of the most robust privacy frameworks in the world, and it includes the principles of data minimization, transparency, purpose limitation, and accountability, as well as the call for greater protection of children's personal data.³⁷

Article 17 of the GDPR, known as the “right to erasure” or “right to be forgotten” is of particular significance. This is important for children, as it allows for the removal of their information when appropriate, and therefore limits the longer-term impact of profiling.³⁸

In contrast to the UK approach of consent, the Age Appropriate Design Code (AADC), also known as the Children's Code, calls for ensuring that the interests of children are at the forefront of design when digital services are likely to be used by children.³⁹ It specifies strong privacy settings as the default, limits the ability to profile and requires transparency about the use of the data.

These are examples of a more systemic approach to accountability and regulation than one that is purely individual responsibility. Their emphasis on privacy-by-design and child-centred governance offers valuable lessons for India's evolving digital regulatory framework.

Reform Proposals

³⁷ Regulation (EU) 2016/679 (General Data Protection Regulation).

³⁸ GDPR, Art. 17.

³⁹ UK Information Commissioner's Office, *Age Appropriate Design Code* (2021).

Digital governance must adopt a proactive approach over a reactive approach to child protection, in a rapidly changing digital environment. Current legal processes are vital, but they tend to focus on the process of addressing harm that has already happened. In today's complex, large and opaque digital systems, especially those for AI-driven decision-making and algorithms, child rights protection needs to be built into the design, development, and regulation of digital technologies. In this context, a comprehensive reform agenda should be based on constitutional values, international child rights standards and new international best practices.

A. Child Rights Educational Resources for Children and Young People

One of the major reforms that would be beneficial is the enforcement of Child Rights Impact Assessment (CRIA) of AI systems, digital platforms, educational technologies, and online services that are likely to impact children. As with environmental impact assessments, CRIAs would involve assessing any risk to children's privacy, safety, autonomy, mental health and developmental interests before bringing them to market by technology developers and platform operators.⁴⁰

These evaluations would foster preventative instead of reactive regulation. Designers and regulators may identify potential harms early in the design process and take measures to prevent those harms from occurring on a large scale. It is important for India to ensure that the impact of digital technologies on children's rights is assessed and acted on before implementation, either in the form of amendments to data protection laws or sector-specific digital governance laws.⁴¹

B. Embedding Privacy-by-Design and Safety-by-Design Principles

Parental supervision and awareness cannot be the sole basis for the protection of children online. With complex technologic architectures in digital environments, children and adults frequently

⁴⁰ UNICEF, *Policy Guidance on AI for Children* (2021).

⁴¹ Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc. CRC/C/GC/25 (2021).

have a hard time understanding the structure. Thus, privacy and safety precautions must be integrated into the technological systems.⁴²

The idea of privacy-by-design suggests the embedding of privacy at the design phase of the product, with reduced data collection, shorter retention periods of the data collected and privacy settings set in default mode, in keeping with the constitutional protection of privacy as a fundamental element of dignity and autonomy in Justice K.S. Puttaswamy v Union of India.⁴³

Likewise, safety-by-design calls for digital services to recognise the risks that could happen to children and take measures to prevent or alleviate them before a product is released. This could involve age-appropriate interfaces, the ability to block direct messages from strangers, improved moderation features, and content filtering mechanisms. If these principles were adopted, child protection would be placed on a system of accountability, not just individual responsibility.

C. Transparency in the Use of Algorithms in the Design and Operation of STEM Curriculum, Instruction, and Assessment

AI algorithms are now shaping children's online experiences, influencing what they see, learn, and do. AI algorithms now dictate what children watch, learn and do online. Recommendation algorithms affect content visibility, social interactions, learning opportunities, and consumer behavior. However, these systems are frequently a “black box” that is hard for users, regulators and even the developers to understand.

There is a need to strengthen algorithmic accountability mechanisms in India that can help mitigate this challenge. Digital platforms should be obliged to report on the functioning of the recommender systems, to carry out independent algorithm audits and to publish transparency reports on content moderation, profiling and automated decision making.⁴⁴

Systems that impact children should be evaluated carefully as algorithmic decisions can have a dramatic impact on cognitive development, behavioral patterns, and mental health. Public

⁴² Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of Ontario, 2011).

⁴³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁴⁴ Sandra Wachter, Brent Mittelstadt & Luciano Floridi, “Transparent, Explainable and Accountable AI for Robotics” (2017) 2 *Science Robotics* 1.

disclosure would help regulators and researchers evaluate discriminatory results, harmful recommendation patterns and inordinate data collection. This is in line with UNESCO's Recommendation on the Ethics of Artificial Intelligence, which highlights the importance of accountability, transparency, and human oversight in the governance of AI.⁴⁵

D. Improving Regulatory and Institutional Capacity

The best law is not enough if it isn't enforced. Institutional shortcomings such as lack of resources, technology and coordination among regulatory institutions are one of the key weaknesses of child protection legislation in India.

News of these shortcomings calls for the creation of specific Digital Child Protection Units in the current system of regulatory and law-enforcement agencies. These units should have experts in Cybersecurity, Artificial Intelligence, Child Psychology, Digital Forensics and Data Governance. They would be tasked with tracking new technological risks, researching issues of digital harm to children, liaising with platforms and helping to implement children's victim support systems.

In addition, there needs to be a greater technological capability and investigative powers of the existing mechanisms like the National Commission for Protection of Child Rights (NCPCR). There would be enhanced implementation and enforcement if there were specialized training programmes for judges, law-enforcement officials, educators, and policymakers.

E. Restricting Behavioural Advertising and Commercial Exploitation

Data collection and processing from children are now a central part of today's digital economies. Numerous online platforms use the behavioural advertising model which gathers a large amount of personal data to forecast and drive user behaviour. Children, in particular, are at risk of being targeted by these practices, as they may not be cognitively developed enough to differentiate between information and persuasive commercial messages.

⁴⁵ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

India should implement more significant regulations on this behavioral targeting to children. These limitations should accord with the global trend of placing a greater emphasis on the need to keep children's data from being used as a tradeable asset.⁴⁶

A regulatory system should be child-centred, acknowledging that some forms of commercial exploitation are not compatible with children's rights to privacy, dignity and development. Hence, more constraints on surveillance-based business models are needed for meaningful child protection.

F. Advancing Digital Literacy and Child Involvement

The law is not enough to solve the problem of digital risk completely. Children are not only expected to be able to access digital resources safely and responsibly, but to be knowledgeable and skilled in doing so. A comprehensive digital literacy programme should therefore be seamlessly embedded in the school curriculum, focusing on privacy awareness, online safety, information critical thinking and responsible online engagement.

Important to note is that children should not only be perceived as passive subjects of protection. Children should be actively engaged in digital policymaking processes, consultations and regulations that impact on their lives, in accordance with the UN Convention on the Rights of the Child, Article 12.⁴⁷

Legitimacy and effectiveness of regulation is increased by participation. Children can bring a different perspective to the digital world that is not being captured by policy and regulation makers. Children's rights-based approach to child protection is reflected in recognising children as active stakeholder and not just a vulnerable user.

G. Towards a Child-Centred Digital Governance Framework

A comprehensive governance framework is needed for child rights protection in the digital world, bringing together legal regulation, technological design, institutional accountability and

⁴⁶ General Comment No. 25 (2021), paras. 95–97.

⁴⁷ United Nations Convention on the Rights of the Child, 1989, art. 12.

meaningful participation. This should transcend the traditional consent approach and take into account the structural circumstances which pose digital risks.

The principles of a child-centred model of digital governance would be privacy-by-design, safety-by-design, algorithmic accountability, institutional oversight, and the participation of children. These principles offer a foundation for making sure technological innovation is in the best interests of children and respects their dignity, autonomy, equality and needs.

Conclusion

Digital childhood is one of the most important socio-legal phenomena of the 21st century. Children are increasingly experiencing, having opportunities to experience and being vulnerable to features and functions of artificial intelligence, social media platforms, algorithmic recommendation systems and data-driven technologies. These technologies offer children great opportunities, but also great risks, relating to issues of surveillance, profiling, privacy exploitation, manipulation, and online harm.

The article has shown how constitutional principles, international child rights standards and comparative frameworks can provide a solid basis for tackling these issues. But new technologies need new ways of protecting personal privacy that are wider than consent and traditional privacy protection methods. Child rights protection should be integral to the design and governance of digital systems.

To ensure child rights protection in the future, the following principles of child-centred digital governance are needed: privacy-by-design, safety-by-design, transparency, accountability, and meaningful participation. This way of thinking acknowledges children as more than victims whose protection is needed, but as active rights-holders who should have dignity, autonomy, and development in digital environments. Re-imagining child rights in this way is key to ensuring that technology advances in the best interests of children and in pursuit of a better and fairer digital future.