

Protection of Children's Rights in the Digital Environment

Anshuman Panda

*Ph.D. Research Scholar, P.G. Department of
Law, Sambalpur University, Prayagraj,
Uttar Pradesh.*

Abstract- The rapid expansion of digital technologies has fundamentally transformed the lives of children by providing unprecedented opportunities for education, communication, creativity, and social participation. The increasing use of social media platforms, online gaming services, educational applications, and artificial intelligence-driven technologies has enabled children to engage with the digital world in ways that were unimaginable a decade ago. However, these developments have also exposed children to significant risks, including cyberbullying, online grooming, child sexual exploitation, privacy violations, harmful content, and data-driven commercial exploitation.

This paper examines the protection of children's rights in the digital environment with particular reference to the Indian legal framework. It analyzes the extent to which constitutional guarantees and statutory measures safeguard children's rights online. The study evaluates the relevance of Articles 14, 19, and 21 of the Constitution of India, along with legislative instruments such as the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Digital Personal Data Protection Act, 2023. The paper also considers international standards established under the United Nations Convention on the Rights of the Child and General Comment No. 25 on Children's Rights in Relation to the Digital Environment.

The paper argues that although India has developed important legal mechanisms for addressing online harms affecting children, the existing framework remains fragmented and insufficient to respond to emerging technological challenges, particularly those associated with artificial intelligence, algorithmic profiling, and platform-based exploitation. Through a comparative examination of regulatory approaches adopted in the European Union and the United Kingdom, the study identifies significant gaps in the Indian framework and proposes measures aimed at strengthening child-centred digital governance. The paper concludes that effective protection of children's rights in the digital age requires a

comprehensive regulatory approach that balances safety, privacy, participation, and development while ensuring that children can benefit from technological innovation without compromising their fundamental rights.

Index Terms: Children's Rights, Digital Environment, Online Safety, Child Privacy, Cyberbullying, POCSO Act, Digital Personal Data Protection Act, Child Protection, Artificial Intelligence, Digital Governance.

I. INTRODUCTION

Digital technologies have greatly enhanced children's lives around the globe. The web is far more than an info outlet today; it is a place for schooling, socialization, entertainment, and self-development. Smartphones, social media, online gaming, education apps, and AI tools have become integral parts of the lives of children today. These technologies offer significant opportunities for learning and participation, but also expose children to new forms of risk.¹

Over the last few decades, children's rights and their relationship to society have completely transformed due to the digital environment. Many activities that traditionally occurred in physical spaces now take place through digital platforms. Children use social networks to talk to other children, attend virtual classes, learn more about health, post opinions on public issues with digital media, etc. Meanwhile, the online landscape has turned into a cultural landscape beset by cyberbullying, data exploitation, online grooming, exposure to harmful content and privacy violation.² These issues lead to significant legal questions: are protections in place sufficient?

In India, this has emerged as an increasingly pressing issue due to the rapid growth of internet access and smartphone usage among children. Children are accessing the digital world at a younger age and many of them are doing so without adequate understanding about the dangers that they may encounter online. While India has enacted laws with child protection, data protection and cybercrime aspects, they have mostly developed to address specific concerns, rather than being built on a children's rights-in-the-digital-environment policy approach. This can leave legal assurances piecemeal and responsive.

Indian law recognises multiple rights that are relevant to children in the digital space, but severe regulatory lacunae remain with respect to privacy online, algorithmic profiling, accountability for platforms, and in respect of novel technological harms. It delves into the theoretical underpinnings of children's digital rights, the surrounding international and domestic legal tools and precedents, as well as current obstacles to the realization of effective rights protection.

¹ Sonia Livingstone & Amanda Third, *Children's Rights and the Internet: From Guidelines to Governance*, 24 *Info. Comm. & Soc'y* 657 (2021).

² UNICEF, *The State of the World's Children 2017: Children in a Digital World* (2017).

II. EVOLUTION OF CHILDREN'S RIGHTS IN THE DIGITAL ENVIRONMENT

Traditionally child protection legislation had been mostly for physical protection, education and child labour and child justice purposes. Digital technologies have brought the dimension of rights beyond the traditional one. The legal system is gradually having to deal with the hazards thrown up by online activities, data collection mechanisms, and automated technologies. Children's rights in the digital environment are founded on a commitment that rights that exist offline should also exist online.³ In fact, however, technology innovations have created new environments in which these rights have to be protected.

The issue of child pornography and exploitation through the Internet was initially a concern for the regulators. As time went on, fears evolved to cover various issues concerning the Internet as a site for bullying, on-line surveillance, commercial exploitation of kid information, manipulative space design approaches, and the psychological impact of too much time on-line. The increasing algorithmic and AI influence has further complexified the situation. To have their content being presented to them if it is recommended by specific systems, to be monitored by behaviour tracking and profiled by automated systems, and without their knowledge of how these systems work, children can be exposed to targeted content.

Another important change is the understanding that children are not just passive users of the digital world but its active users who can access and use digital products without child protection barriers. There are two elements of contemporary children's rights vocabulary that stress protection as well as empowerment. Children need to be protected from harm but they also have the right to access information, to voice opinions, to engage in cultural life and go through technological innovation. Protection and autonomy and participation should be balanced in the legal framework.

The digital world and the challenges it offers are also trans-national. There are online platforms with a global footprint, and regulatory systems, which are mainly territorial. harmful content, online predators, and cross-border data transfers frequently cross the line, complicating enforcement. International collaboration has consequently been a key focus of safeguarding kids' rights in the digital world.

III. INTERNATIONAL LEGAL FRAMEWORK

The United Nations Convention on the Rights of the Child (UNCRC), adopted in 1989, is the most crucial instrument internationally concerning children's rights, viewing children as rights bearers and requirements from states for their survival, development, protection, and participation. UNCRC was developed prior to the extensive use of the internet but its core principles have a

³ Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, ¶ 4, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).

strong bearing in digital settings.⁴ There are a number of aspects that can also be implemented in online activities. The rights of freedom of expression (Article 13), privacy (Article 16) and access to information that is conducive to the welfare of the child (Article 17) are acknowledged. These rights remain unaffected, whether offline or online. In 2021, the United Nations Committee on the Rights of the Child released General Comment No. 25 on Children's Rights in Relation to the Digital Environment, which offers authoritative advice on the Convention's implementation in digital contexts.⁵ The General Comment's aim is to "strengthen efforts to ensure that digital technologies can foster children's development and help to safeguard children from exploitation, abuse, privacy threats, and harmful content.

In General Comment No. 25, the Committee acknowledges that children's learning, information-sharing and social engagement can be greatly enriched by digital technologies. It also raises awareness about threats that exist with the sharing of commercial data, algorithmic profiling, cyberbullying and sexual exploitation online.⁶ The document urges the states to follow a child-centred governance approach and to do so, starting with working with the best interests of the child as a guiding principle in digital governance. Increasingly, international bodies have emphasized the need for cooperation between governments, technology firms, educational establishments and civil society organisations in the digital age to ensure child protection. Ensuring child safety is not a one-size-fits-all endeavor, and cannot be entrusted solely to parents and individual users. Rather, the child-sensitive design and safety mechanisms shall be made (again) available in digital platforms.

IV. DIGITAL RIGHTS OF CHILDREN: PRIVACY, PROTECTION, PARTICIPATION, AND DEVELOPMENT

Children's rights in the digital environment can be understood through four interconnected dimensions: privacy, protection, participation, and development. This is not only one of the most significant digital rights, but also one of the most elementary. Children are leaving a large volume of personal data while using the internet. It can include data about behaviour, preferences and location, which many of the social media platforms, games apps, search engines and educational technologies will gather. This can mean raw data is collected and their identities soundly monitored and profiled, potentially leaving them vulnerable to commercial use, retail television monitoring, and/or surveillance.⁷ Privacy protection thus implies that there must be legal protections and safeguards in place in addition to good technology design.

⁴ Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

⁵ Committee on the Rights of the Child, *supra* note 3.

⁶ *Id.* ¶¶ 12–18.

⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

The right to protection includes the rights to freedom from violence, abuse, exploitation, and harmful content. The advent of digital technologies has led to novel and distinct forms of victimisation such as cyberbullying, online grooming, identity theft, and the sharing or posting of child sexual abuse material. The key to effective protection is early action and regulatory safeguards, platform accountability, and easy reporting avenues. Children have other digital rights as well, namely to participate. The internet allows children to learn, communicate, post or issue voices and to get information from many sources. Digital technologies, used in an appropriate and responsible manner, can empower democratic participation and education. Excessive restrictions can have a detrimental impact on this and reduce opportunities of children's self-expression. Finally, the right to development affirms the centrality of digital technologies in today's learning, creativity and socialization. Use of digital resources is increasingly affecting learning outcomes and future opportunities. This poses a specific challenge for States to safeguard children when the internet is rife with potential harms, as well as ensuring that they have equal access to safe and positive digital experiences.⁸

These four dimensions are interrelated. Overemphasis on protection can lead to reduced participation and access, and unprotected participation can lead to serious risks for children. A harmonious legal system should therefore aim at balancing the child protection measures with the scope for technological development and digital inclusion. Child rights protection should not only be based on legal categories, as digital technologies are changing. The Internet, and digital technologies in general, are now an intrinsic part of childhood, and this must be acknowledged by contemporary legal systems. Protecting children's rights online will therefore not be a discrete legal goal but essential to overall efforts to protect children's rights.

Part II: Constitutional and Statutory Protection of Children's Rights in India

There is a mix of constitutional and statutory protections for children's rights in the digital environment in India. The Constitution of India has been penned years before the advent of digital technologies, but its provisions offer a valuable framework for safeguarding children against online harms and ensure that they are able to benefit from the technology. In addition to constitutional rights, there are several laws that seek to address certain risks including online sexual exploitation, violation of privacy, and cyber crimes.⁹

Constitutional Protection

There is no explicit mention on digital rights in the Constitution of India. However, there are some basic rights that apply online and to children as well. The equality before the law and equal

⁸ UNICEF, Policy Guidance on AI for Children (2020).

⁹ INDIA CONST. arts. 14, 19, 21.

protection of the laws is guaranteed in Article 14. In the digital context, this provision is similarly grounded in children's right to equal opportunities with technology and online platforms and the need to uphold children's rights against discriminatory forms of engagement with technology. Article 19(1) (a) states that everyone has the right to free speech and expression. The Internet is an influential face-to-face medium where children spend time communicating, learning and sharing their beliefs. Digital technologies provide access to educational, cultural and social opportunities for children which may have been unavailable to them before. Therefore, in order to ensure meaningful participation in contemporary society, online expression protection is essential.¹⁰

The rights and freedoms of children in terms of their rights in the digital sphere have the best constitutional foundation in Article 21. The Supreme Court has consistently held the Right to life/Right to personal liberty extremely wide, to take care of dignity, autonomy and privacy. In the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, the Court has declared privacy as a fundamental right guaranteed under Article 21, while the incident is not about children, the principles laid down are relevant in case of collection, processing and storage of children's personal information by digital platforms.¹¹ Further, the state policy to be followed as per the Directive Principles of State Policy confirms the commitment of the constitution towards child welfare. Article 39(e) requires the State to protect children from abuse, while Article 39(f) seeks to ensure that children develop in conditions of freedom and dignity. These principles offer normative backing for improved legal efforts against on-line exploitation, cyberbullying and dangerous online content material.¹²

Statutory Framework

The legal framework for protection of children in India via online sources is spread across a number of legislations. The most important Act that has been enacted is the Protection of Children from Sexual Offences Act (POCSO Act), 2012. The intent of the legislation is to comprehensively legislate for sex offences involving children. The provisions were originally intended to deal with acts of sexual offence but the use of provisions has expanded over time to apply to sexual offences that happen electronically, like online grooming, online sexual harassment and circulation of child sexual abuse material.¹³ The Information Technology Act, 2000, is another vital legislation. The main framework of Indian cyber law is the Act and provisions specifically relating to 'unlawful contents' are provided in this Act. Section 67B, which makes it an offence to 'publish, transmit, browse, download or have possession of any material' that depicts children in 'sexually explicit acts' is of particular importance. This a recognition in the law of the serious nature of child exploitation that can be aided by digital technology and for which special legislative measures are needed.¹⁴ Digital Personal Data Protection Act, 2023, is a major step ahead for the protection of

¹⁰ Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.

¹¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

¹² INDIA CONST. arts. 39(e), 39(f).

¹³ Protection of Children from Sexual Offences Act, No. 32 of 2012, INDIA CODE (2012).

¹⁴ Information Technology Act, No. 21 of 2000, § 67B, INDIA CODE (2000).

children in terms of their privacy. The Act provides that a child is defined as someone under the age of eighteen and requires parental verification of consent for processing personal data that involve children. The Act also restricts behavioural monitoring, tracking, and targeted advertising directed at children.¹⁵

Further, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 prescribe certain obligations to be fulfilled on the part of the intermediaries and the social media platforms. Examples of these obligations are grievance redressal processes, due diligence processes, and working with lawful authorities. While not particular to children, the Rules have been designed to help online environments become safer and more responsive to the detrimental and unlawful content.¹⁶ These have failed to create a single comprehensive framework existing legal framework, even with these measures. Different statutes address specific risks without establishing a unified approach to children's rights in the digital environment. Consequently, important issues such as algorithmic profiling, age verification mechanisms, and AI-driven harms continue to present regulatory challenges. These concerns highlight the need for a more comprehensive and child-centred legal framework capable of responding to rapidly evolving technologies.

Part III: Contemporary Challenges and Threats to Children's Rights in the Digital Environment

Children are exposed to many risks in digital space despite the existence of constitutional and statutory protections. New opportunities in education and socialisation – new harms created by technological developments and not easily controlled by the law. Much of these are transnational, technologically advanced and constantly changing. Consequently, achieving good protection of children's rights needs to be done with better awareness of the challenges which become part of the digital environment today.

Cyberbullying and Online Harassment

Cyberbullying is now one of the principal threats that kids have to face online. Cyberbullying can take place at any time, and has the potential to network a bullying incident to a much broader audience via social media, user-to-user messaging applications, and forums online. Children may experience harassment, threats, humiliation, impersonation or disclosure of personal information without consent.¹⁷ Cyberbullying can have lasting consequences. Research has shown that long-term victimization by cyberbullying can lead to anxiety issues, depression, low self-esteem, social withdrawal, and academic problems in minors, as well as other health issues and behaviors such

¹⁵ Digital Personal Data Protection Act, No. 22 of 2023, §§ 9–10, INDIA CODE (2023).

¹⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, Part II, sec. 3(i) (Feb. 25, 2021).

¹⁷ UNICEF, The State of the World's Children 2017: Children in a Digital World (2017).

as self-harm and suicidal.¹⁸ A further obstacle in the problem is the permanency of the digital content, as all the negative content will still be available long after the initial incident.

Presently, India does not have a solid and enacted policy specifically targeting cyberbullying of children. General provisions covering harassment, defamation, criminal intimidation or cyber offences are relied on by victims. These provisions can offer remedies in some circumstances but do not sufficiently capture the particular dynamics of online harassment experienced by children. As a result, prevention, awareness building and responsibility on the platforms remain key pillars in protection.

Online Grooming and Sexual Exploitation

Online grooming is one of the most serious risks of the online world. Grooming is where an offender gets to know a child for the purposes of sexual exploitation. Crimes such as bullying, harassment, and exploitation also are able to take place with child victims on social media, gaming forums, messaging programs and anonymous chat communities.¹⁹ Online grooming often times goes on for long durations. To do this, offenders might use emotional support, gifts, compliments or false identities with children to make them feel vulnerable and gain their trust before trying to exploit them. Bullying is hard to identify on the internet. Grooming behaviors are not obvious to children, especially if communicated in a friendly or supportive way.

Another area of concern is the spread of child sexual abuse material (CSAM). Modern digital technology has facilitated the creation, storage and rapid and widespread circulation of offensive material from one jurisdiction to another.. When once this material is uploaded online, total removal can be quite complex. A victim can thus suffer long-lasting injuries after the first abuse.²⁰

India has made substantial strides in the matter and the POCSO Act along with Section 67B of the Information Technology Act. But the enforcement problems remain, as the Internet allows for cross-border servers and encrypted communications and illegal materials can be disseminated very quickly. There needs to be a team effort among law enforcement agencies, on the internet, among social media websites and from around the world.

Privacy Violations and Data Exploitation

The collection and treatment of children's personal information is a key challenge in the digital era. The modern digital platforms collect a lot of information on the behaviors and interests of their users, their site navigation patterns, their location, and their interactions, among others. Children

¹⁸ Sameer Hinduja & Justin W. Patchin, Cyberbullying: Identification, Prevention, and Response, 49 Cyber Safety Rev. 11 (2021).

¹⁹ Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, ¶¶ 82–84, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).

²⁰ Information Technology Act, No. 21 of 2000, § 67B, INDIA CODE (2000).

sometimes provide information that is personal without being aware of the consequences of data being used, stored, and shared.²¹ As the use of data-driven business models has risen, there has been a growing concern on commercial exploitation. Targeted advertising and behavioural profiling are important sources of revenue for many online services. Sophisticated algorithms can forecast choice and steer user behavior. Children are very vulnerable as they might not have the maturity to assess persuasive design techniques and promoted content.

Concern over privacy has been brought to the fore in the case of educational technology platforms as well. Data regarding student learning experiences has been massively gathered with the widespread use of digital learning tools. Such technologies have the potential for improvement in child access to education; however, poor education protection could lead to children being subjected to unauthorized data sharing, security breaches or intrusive monitoring practices.²² Digital Personal Data Protection Act, 2023 is a significant legislation by introducing specific protections for children's data. However, there are doubts about the implementation, enforcement, and effectiveness of parental consent processes. In addition, uncertainties exist about the way information collected from children is going to be used, for more complex purposes and applications, with emerging technologies like Artificial Intelligence.

Harmful Content and Mental Health Risks

The Web contains vast amounts of information, some of which can be of a beneficial nature for educational and developmental purposes. Children are also seeing the bad or got to something at the time, though. This can include violent content, pornography, self-harm content, hate speech, extremist propaganda, misinformation or content relating to harmful conduct. Children's emotional and psychological development may be impacted by exposure to harmful content.²³ Teens or young adults who are more susceptible to such manipulation may have difficulty identifying accurate information from misinformation or manipulation. Social media sites tend to have a recommendation algorithm that is used to find items that will keep you engaged, potentially propagating sensational or harmful content. The conversations about children's rights to the use of technology have increasingly turned to mental health issues. High rates of social media use have been shown to be linked to anxiety, negative thoughts about body image, sleep problems and lack of social contacts. The never ending need to be "on the internet" can bring emotional stress and low levels of self-confidence. Digital technologies are not an inherently bad thing, but features of platforms can promote extended ends and addictive behaviours.²⁴

²¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

²² UNICEF, Policy Guidance on AI for Children (2020).

²³ Convention on the Rights of the Child, Nov. 20, 1989, art. 17, 1577 U.N.T.S. 3.

²⁴ Sonia Livingstone & Alicia Blum-Ross, Parenting for a Digital Future: How Hopes and Fears About Technology Shape Children's Lives 43–47 (2020).

Such challenges illustrate that it is impossible to restrict children's rights protection to prevention of criminal behavior. The design and use of digital platforms must also have developmental and psychological consequences, which should be taken into account in regulatory practice.

Artificial Intelligence, Deepfakes, and Emerging Technologies

Emerging technologies open new problems which are not catered by current legal frameworks. AI algorithms are shaping the media stories viewed by kids, the ads they are exposed to, and suggestions the programs use to curate what kids see and experience online. AI-driven recommendation systems increasingly influence the content children view online and the information they encounter. Children may not recognise that algorithmic systems are influencing their behaviour, and this has led to concerns for its autonomy, transparency and accountability.²⁵ One growing concern is the use of AI-generated deepfakes. Deepfakes involve synthetic media that can realistically depict individuals saying or doing things that never occurred. Children may become victims of manipulated images or videos used for bullying, harassment, reputational damage, or sexual exploitation. Existing laws do not comprehensively regulate all forms of deepfake-related harm, particularly where content does not clearly fall within traditional criminal categories.

Virtual reality environments and emerging metaverse platforms create additional concerns. These technologies blur distinctions between physical and digital interactions, potentially exposing children to new forms of harassment, manipulation, or exploitation. Regulatory frameworks designed for conventional internet platforms may prove inadequate in addressing harms occurring within immersive digital environments. The rapid pace of technological innovation creates a persistent challenge for lawmakers. Legal systems often respond only after harms become widespread, resulting in a gap between technological development and regulatory protection. Consequently, a forward-looking approach is required—one that anticipates emerging risks rather than merely reacting to them after significant harm has occurred.

The challenges discussed above demonstrate that children's rights in the digital environment face threats that extend beyond traditional legal categories. Cyberbullying, online exploitation, privacy violations, harmful content, and AI-driven risks collectively reveal the limitations of existing regulatory mechanisms. While India has established important legal safeguards, the evolving nature of digital technologies necessitates stronger institutional responses, enhanced platform accountability, and a comprehensive child-centred regulatory framework capable of addressing both present and future harms.

Part IV: Comparative Perspectives, Regulatory Gaps, and Recommendations

Comparative Perspectives

²⁵ UNESCO, Guidance for Policy-Makers on AI and Children (2022).

In recent years, children's experiences continue to be influenced by digital technologies, leading several jurisdictions to adopt specific regulatory interventions to ensure protection of children online. A comparative analysis demonstrates that child-centred digital governance is increasingly recognised as an essential component of modern legal systems. It is the European Union that has become a global leader in the protection of digital rights via the General Data Protection Regulation (GDPR). The GDPR has special rules about the processing of personal information about children, particularly in regard to the obtaining of consent, and includes guidance on ensuring that information is presented in a way that is understandable to children.²⁶ It bestows the rights of access, correction and deletion on individuals. The European vision goes beyond privacy legislation, however, and more and more includes the notion of “safety by design.” Digital platforms are expected to have protective mechanisms within their services from the beginning rather than having to import these from outside because of parental oversight. This method acknowledges that children shouldn't be responsible for deciding on complicated technological risks on their own.

The Age Appropriate Design Code or the Children's Code, is an innovative step in the United Kingdom, where the Code clearly stipulates that online services that are likely to be used by children are designed with their best interests in mind. It has a high default setting of privacy, restricts data collection and minimizes the use of methods which persuade children to provide too much information.²⁷ One of the key elements of the Children's Code is that rather than targeting user-level behavior per se, it specifies the design of the platforms themselves. In addition to user actions, the effects of a technology are defined as harmful in the framework, where these effects are not only due to user actions. As a result, service providers are expected to foresee risk and establish safeguards in advance of any risk.

The international processes indicate a change from reactive regulation to preventive governance. Notions of accountability, transparency and child centred design are more and more placed at the center. These measures can serve as useful inputs in the quest to build India's regulatory regime.

Regulatory Gaps in India

While there has been significant legislative progress, India's legal system to safeguard children's rights in the digital landscape is still incomplete. While various laws deal with particular harms, there is no specific legislation to cover children's digital rights as a separate legal category.²⁸ There is 1 major weakness here with the platforms. Current legislation does have some requirements for intermediaries, but not detailed requirements for the design of the products, making

²⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

²⁷ Information Commissioner's Office, Age Appropriate Design Code: A Code of Practice for Online Services (2020).

²⁸ Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Information Technology Act, No. 21 of 2000, INDIA CODE (2000); Protection of Children from Sexual Offences Act, No. 32 of 2012, INDIA CODE (2012).

recommendations using algorithms, or ensuring that minors are protected from manipulative online activities. This means that children continue to be at risk from systems that have more of a focus on getting users involved in the business than looking after their well-being.

One of the other issues is age verification. Some websites have set age minimums, but there is not necessarily consistency in practice. Services for the older users may be accessible to children too using false information at the registration process. Interestingly, often there are services for the older users which can be obtained by a child with wrong information during registration. Lack of reliable verification mechanisms and privacy respecting safeguards lowers the result of currently present safeguards. Unfortunately, controlling artificial intelligence is another issue. AI recommendation systems are increasingly shaping children's internet use, by choosing what children see. These systems can unintentionally convey negative content, stereotypes, or oversaturation. There is very little law-specific information in India on the current use of these technologies with children.²⁹

The lack of enforcers reduces the legal protections. Cyber crimes are often international in nature, perpetrated by unknown actors, and technologically complex. Due to practical challenges in identification, preservation and cooperation from abroad, investigators may be obstacles. Legal safeguards as a result may, therefore, be written but hard to implement. Last, but not least, there's always the issue of awareness. Most parents, children and teachers are not well-versed in the risks an online environment presents, privacy procedures or legal available (and applicable) solutions. Protection can only be realized through legislation, but it has to be supported by informed engagement of all parties to children's digital lives.

V. RECOMMENDATIONS

Solutions to the protection of children's rights in the digital world should follow a multi-dimensional approach involving legal measures, capacity building of institutions, technological solutions and educational measures.

First, India may want to have a more complete approach to child online safety which brings together existing safeguards and, at the same time, mitigates emerging technologies risks. The legislation should specifically outline platform's roles, include requirements for platforms to put the child first when designing products and services, and ban algorithmic exploitation.³⁰

Second, it must be obligated to digital platforms to pursue “safety-by-design” principles. Other privacy-preserving settings should be set to the default place; behaviours and behavioral designing practices should be investigated more carefully for children. Service providers should also regularly review the impact of their technologies on children, while performing risk assessments.

²⁹ UNESCO, Guidance for Policy-Makers on AI and Children (2022).

³⁰ Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).

Third, greater regulatory oversight is required for AI systems that affect children. Algorithmic systems must not infringe on children's rights and wellbeing, and this must be addressed through transparency, independent auditing and accountability.

Fourth, the digital literacy programmes should be embedded into the curriculum of education. Kids need to have hands-on information about online safety, privacy protection, and how to prevent cyberbullying, as well as teach them about responsible use of the Internet. Parents and teachers should also be the focus of similar campaigns of awareness.

Finally, a greater synergy among government, technology firms, education and civil society is needed. Selected digital risks are in a state of constant change and not everyone can respond to them in isolation. The involvement of multiple parties in governance arrangements offers a flexible, responsive approach to the protection of children's rights in a very complex technological landscape.

VI. CONCLUSION

Today, the digital world has revolutionized the lives of children making education, communication, creativity and participation like things that have never happened. It has simultaneously created new risks which defy current child protection practices. Children's rights are now also at stake online, through the use of emerging technologies, including AI; harmful content; violation of privacy and cyberbullying. The government of India has laid a strong groundwork to safeguard children in its Constitution, pursuing legislation like POCSO Act and the Information Technology Act, as well as the Digital Personal Data Protection Act, 2023. These gestures are part of a trend toward increasingly advocating for the need to tackle digital harms. Despite these developments, India's legal framework remains fragmented and often struggles to respond to rapidly evolving technologies. A more comprehensive child-centred regulatory framework is required to address emerging challenges such as algorithmic profiling, AI-driven harms, deepfakes, and platform accountability. Protecting children's rights in the digital environment is not merely a matter of cyber regulation; it is an essential component of protecting children's rights in the twenty-first century.