Page 1486 – 1503 **DOI:** *https://doij.org/10.10000/IJLMH.1111602*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Growing Up Online: Legal Frameworks, Children's Rights, and the Regulation of Social Media in Contemporary India

ANANYA BHANDARI[1] AND AMRUTA NERLIKAR[2]

ABSTRACT

Each and every State carries the key responsibility ensuring the protection of children, who are widely considered as one of the most vulnerable sections in society. This concern received global recognition especially after the adoption of the UN Convention on the Rights of the Child, leading to establishment of key principles including equality, the right to life and development, and making their best interests the most important factor in every decision affecting them.

The sudden increase in the growth of digital technologies and internet-based platforms has altered how young people access data, learn, and interact socially. While the digital world provides many opportunities for learning, creativity, and interaction, it also puts children at risk of problems like cyberbullying, online exploitation, misuse of personal information and loss of privacy.

The COVID-19 pandemic further brought these concerns into attention. With the sudden shift to online modes of learning and communication, it became vital for children to adjust quickly to new forms of interaction which thereby, revealed gaps in existing systems and highlighted the need for stronger rules and laws to protect children in both physical and digital spaces.

This paper sheds some light by deeply analysing the relationship between digital rights and youth protection, underlining the necessity for an approach that is balanced and ensures safety while enabling children to exercise their rights in the digital environment. It supports a system based on international standards that can create a safe and inclusive digital space which ultimately helps in their growth and well-being.

Keywords: Digital Rights, Youth Protection, Data Privacy, Data Protection Laws (DPDP Act, 2023), Child Online Safety

I. INTRODUCTION

In contemporary times, life in India is being rewritten by the digital world. It is present in the

[1] Author is a Student at Symbiosis Law School, Pune, India.
[2] Author is a Student at Symbiosis Law School, Pune, India.

 [ISSN 2581-5369]

way that we talk to each other, how we learn, how we are being entertained, and how we interact with the government. The internet has moved from being a luxury to something that has occupied an integral place in our society due to its nature of making everything easily accessible.

But the real face of this change is the children, who are in turn the assets of our society. They are not just users; they are one of the fastest growing section in this digital space. With smartphones and data, now reaching even the most remote corners, children are connected in ways their parents never were. While this world offers them incredible ways to learn and grow, it also opened the door to a new set of complex risks that we, need to face with urgency and constant care.

The digital world has been successful in dissolving the walls of the family home, or when simply stated, in making the line between a child's private life and the public eye incredibly thin. For kids in this generation, being online is not just a hobby rather it is how they learn, play, and stay connected. It is woven into the fabric of their daily existence.

The real trouble is that while most apps claim to have 'digital security measures' like age verification[3],, these systems are often easy to evade in reality. This means children frequently wander into those corners of the internet without actually grasping the true horrifying, long-term consequences of their actions in the form of digital footprints. It leaves them wide open to different forms of modern dangers, from the cruelty of cyberbullying and 'catfishing' to more predatory risks like grooming and identity theft. Perhaps most heartbreaking is the global rise in online exploitation, a threat that does not care about the age and background of the child.

But the risks are not always loud or obvious. There is a quieter, more subtle influence that plays a central role in all of this: **algorithms**. These automated systems are designed to track an individual's habits and feed them targeted content. Without even realizing it, the perceptions, body image, and behavior of a child are being shaped by these which highlights why we need to create environments that are genuinely safe for them, rather than just checking a legal box.

Finally, we have to look at our own habits through the lens of **'sharenting.'**[4] Even when parents post out of pure love and pride, sharing every milestone and cute moment online can unintentionally strip a child of their privacy before they are old enough to have a say in it.

[3] Shariff S and Johnny L, "Child Rights in Cyberspace: Protection, Participation, and Privacy" (De Gruyter, January 29, 2016) https://www.degruyterbrill.com/document/doi/10.3138/9781442687615-012/html accessed March 28, 2026)

[4] Tepelena, I. (2025). The Legal Framework of Sharenting: Protecting Children's Rights in the Digital Age. *Interdisciplinary Journal of Research and Development*, *12*(1 S1), 93-93.

 [ISSN 2581-5369]

Protecting a child's digital footprint is not just a formality; it is about making sure their future well-being and dignity always come first.

It is also pertinent to note that the digital sphere should not be viewed solely as a place of risk; it is also a means of empowerment. It provides children with opportunities to express themselves, access academic resources, build digital skills[5], and participate in civic life. For many, especially those in developing regions, access to digital tools plays an important role in reducing educational and social disparities. The real obstacle, therefore, is not to limit children's use of digital spaces, but to ensure that the access remains a place which is safe and supportive of their development and well-being.

The concept of protection of youth in today's digital world must not be taken lightly as a one-man job since it requires a collaborative, coordinated and multi-layered effort[6]. Governments play a central role in all of this, as their primary goal involves building the legal frameworks which includes adoption and subsequent implementation of strict data privacy laws and safety regulations that hold all these technology companies or giants accountable for their practices. However, these legal measures are insufficient when alone. Technology companies must adopt some approach by integrating safety features directly into their platforms and have reliable systems in place to filter out harmful content before it reaches young users.

Furthermore, educational institutions such as schools and families also play a integral role in helping children develop digital literacy which goes beyond knowing how to use these devices as it includes understanding online information, protecting their privacy, and identifying harmful risks. When children learn these skills, they can not only make better choices but also use the internet more carefully. It is as much as the duty of parents and guardians, as of the government, to ensure they guide and support their children appropriately while also respecting their independence, helping them build healthy digital habits without restricting their rights.

The COVID-19 pandemic further emphasized the growing significance of digital technology[7] in the lives of several children. with schools closed and physical face to face interactions being limited, children increasingly depended more on online platforms. While this greatly helped them stay connected and continue their learning, it also increased children's exposure to online

[5] Abdul Aziz N, "Child's Right to Free Flow Information via Internet: Liability and Responsibility of the Internet Service Provider - ScienceDirect" (Child's Right to Free Flow Information via Internet: Liability and Responsibility of the Internet Service Provider - ScienceDirect, April 19, 2012) https://www.sciencedirect.com/science/article/pii/S1877042812008154 accessed March 29, 2026

[6] Livingstone S, Third A. Children and young people's rights in the digital age: An emerging agenda. New media & society. 2017 May;19(5):657-70. https://journals.sagepub.com/doi/abs/10.1177/1461444816686318

[7] Virat S. Child Rights in the Digital Environment. Issue 1 Indian JL & Legal Rsch.. 2023;5:1.

risks and led to increased gaps in access to digital resources amongst many.

A. Complexities in Safeguarding Children Online

The risks that could be encountered within the digital space are further heightened because of the anonymity and operation taking place across different countries, which could pose as a means of advantage for a lot of groups of people, while as a disadvantage for the vulnerable population, particularly children. Reports from international organizations indicate towards a sharp rise in the number of various child sexual abuse material (CSAM)[8], representing the seriousness of the issue. Such exploitation has severe consequences, as it raises questions over not only the immediate safety of children but also have a huge impact on their long-term mental, emotional, and social well-being, urging for stronger measures for child protection.

Around the world, there have been a lot of collaboration and hard work for the prevention of violence against kids, especially with the **INSPIRE framework[9]**. This was a huge effort led by groups like **WHO** and **UNICEF** to mix better laws with social awareness, safe spaces, and real support for parents and teachers alike.

But as good as that sounds on paper, the reality is a lot different especially in developing nations it is not as easy as it might seem initially. In a country like **India**, the intentions are there, but the execution often not up to the mark. We struggle with policies that do not always reach the people they need to and a lack of coordination with other states. Additionally, there is a constant, difficult tug-of-war between ensuring safety of a child while also respecting their right to privacy.

A national legal framework offers guidance, but individual states have the authority to plan[10] and also implement specific changes as they deem necessary. This approach encourages innovation, allowing states to develop new child safety initiatives that can be adopted at the national level If they prove to be successful. Recently, some states have taken steps to strengthen these measures. However, a major problem is the lack of a consistent and effective safety system across the country.

Eventually, the main challenge lies in reaching at a middle point or in simple words, striking a

[8] Gupta.S., "*Child's Right in Cyberspace: A Critical Analysis of Protection and Privacy Under the Indian Legal System"*, 4 Int'l J. Legal Sci. & Innovation 148 (2021), https://www.ijlsi.com/wp-content/uploads/Childs-Right-in-Cyberspace.pdf (last visited Mar. 31, 2026).

[9] Nawaila MB, Kanbul S, Ozdamli F. A review on the rights of children in the digital age. Children and Youth Services Review. (2018), Nov 1;94:390-409. https://www.sciencedirect.com/science/article/pii/S0190740918305851

[10] Gudla S. Digital Distress, Legal Blindness: Gaps in Consent Mechanisms for Indian Teenagers by the Digital Platforms. Legal Blindness: Gaps in Consent Mechanisms for Indian Teenagers by the Digital Platforms (September 10, 2025). 2025 Sep 10. file:///C:/Users/91996/Downloads/ssrn-5468066.pdf

balance between protection and empowerment. It might seem a bit of a tightrope walk. If we are stringent with children and cut their access off from the internet, we end up holding them back from the very tools they need to learn about in order to succeed in the modern world. But if we just leave them to without any rules, we are leaving them wide open for being exploited.

The real aim is finding a middle ground. We need to respect that kids of today are more active, smart participants in the digital world, but we also need to ensure their safety while teaching them how to navigate the web safely on their own.

A. Research Objectives

- To assess whether these regulations are capable of ensuring accountability, transparency and timely redressal of disputes.
- To examine the notion of digital rights and its relevance to children and adolescents in the modern digital environment.
- To identify challenges that one might face as an obstacle in the proper implementation, such as age verification, digital inequality and platform accountability.
- To evaluate the efficacy of various legislations, particularly in addressing risks arising from algorithm-driven content.
- To critically examine how digital rights have developed as an extension of basic constitutional guarantees, and to assess the applicability to children within the digital environment.

B. Research Questions

- Whether India's Digital Personal Data Protection Act, 2023 is adequate in safeguarding children's privacy online?
- Whether the federal framework of governance in India creates disparities in the implementation of laws concerning children's online safety.?
- What reforms should be made to Section 79 of the Information Technology Act to impose proactive duties of care towards child users?
- How Indian laws can balance protection of children form digital harms while preserving their right to participation and digital empowerment?
- To what extent are the age verification mechanisms on Indian Social media platforms effective in protecting minors?

 [ISSN 2581-5369]

C. Methodology

The study was conducted using Doctrinal method. Most of the information was easily available Online. For the research, a comprehensive study was done by using online sources such as journals, articles and newspapers. The study is organized with the help of secondary data collected through different online articles, publications, judicial precedents and websites including JSTOR, SAGE JOURNALS, MANUPATRA, SCC ONLINE amongst various others.

II. CRITICAL ANALYSIS

A. The Dynamic Nature of Child Welfare in the Digital Environment

Digital rights, in very simple terms, can be understood as our basic human rights when applicable to the online world. These include important freedoms like privacy, freedom of expression, access to information, and protection of personal data. Today, these rights have become vital part of our system since it ensures that people are able to participate actively and safely in the digital world.

When we look at it customarily, the concept of child rights has only focused on protection from physical harm, neglect, and exploitation, alongside ensuring basic access to education, healthcare, and other welfare related services.

Moreover, as society heads towards a fast-pacing digital transformation, these principles need to be reconsidered. The online world introduces new types of risks that are often hidden, complex, and difficult to control. Therefore, existing laws and systems must evolve and adapt to deal with these challenges effectively.

As far as children are concerned in digital environment, many organizations collect children's personal information when they use social media platforms like Facebook, Instagram amongst various others. Unlike adults, children are often not aware that their personal data[11] is protected under the ***right to privacy***. Because of their young age, their online activities are frequently monitored by parents, schools, and even the state, which may bear some negative consequences for them in the future in the shape of digital footprints.

B. Key Insights from the Cannataci Report

The challenges that might be faced during parenting especially in the modern age and time, were famously addressed by **Joseph Cannataci** (UN Special Rapporteur on the Right to

[11] Milkaite I, Lievens E. Children's rights to privacy and data protection around the world: Challenges in the digital realm. European Journal of Law and Technology. 2019 May 16;10(1). https://www.ejlt.org/index.php/ejlt/article/view/674

Privacy) in a report to the Human Rights Council[12]. His findings stated the following:

- **Impact on Intelligence:** How constant digital engagement and algorithmic targeting can shape a child's perception of their surroundings and world in general.
- **Privacy Erosion:** Technology today can easily interfere with children's private lives, often before they are mature enough to understand or consent to it.
- **Shared Responsibility:** Protecting children or the 'burden of protection' does not naturally fall upon solely on parents of the concerned child. While families face challenges in raising children in a digital world, the State also has an important role in creating and enforcing laws to keep them safe.

This is where the principle of the ***'best interests of the child'*** comes into play as it forms a fundamental part of international law and gained importance through the UN Convention on the Rights of the Child. As provided under **Article 3(1)[13],** it requires that a child's well-being be treated as the foremost consideration in all decisions made by the state, families, or institutions.

Rather than being a narrow legal rule, the 'best interests' principle acts as a lens through which all other rights including the **right to privacy[14]** are interpreted. The primary goal lies in the protection of physical, and rational integrity of the youth, ensuring their human dignity is respected both in the real and digital world.

This concept draws significant attention and has been widely discussed in academic and legal studies due to the nature of its importance. Scholars and courts have tried to understand how it should be applied in real life situations to truly benefit children as they are the most prominent and active web users. However, one major issue is that the Convention does not clearly define specific factors for deciding what is in the best interests of children as also pointed out by Michael Freeman[15].

To address this, the UN Committee on the Rights of the Child issued **General Comment No. 14 in 2013**, which provides guidance on applying this principle[16]. Even then, it does not give a fixed list of rules. Instead, it explains that the best interests of the child is a flexible and evolving concept. It offers a framework to help in decision-making but does not prescribe a single answer,

[12] United Nations Office of The High Commissioner, Children's right to privacy in the digital age must be improved, (July 2021).
[13] Kravchuk N. Privacy as a new component of "the best interests of the child" in the new digital environment. The International Journal of Children's Rights. 2021 Feb 12;29(1):99-121.
[14] Ibid
[15] Ibid 5
[16] Ibid

 [ISSN 2581-5369]

as what is best for a child may vary depending on the situation and over time.

Unlike the UN Convention on the Rights of the Child, the European Convention on Human Rights does not directly mention the best interests of the child. However, the European Court of Human Rights has dealt with this idea in many cases related to rights of children. The Court has stated that there is no fixed list of factors to decide what is in a child's best interests, as it depends on each individual situation. It also clarified that a child's interests are not always the same as those of the parents and, in some cases, the interests of a child can be more important than those of the parents. Even without a pre-determined list, certain things are generally considered important for children, such as their health, development, family relationships, and stability in their living environment. These are usually treated as part of the child's best interests unless specific circumstances suggest otherwise.

The courts have recognized that internet can pose serious risks to basic rights, especially the right to privacy. Because of this, privacy is now seen as an important part of a child's best interests in the digital world. As discussed above, it is the primary duty or responsibility of both the parents/ guardians of children as well as the state to ensure a safe environment for everyone including this vulnerable population when surfing or exploring online. The Convention also clearly states that a child's best interests should be **'primary consideration.'** This wording was chosen carefully[17] to give some flexibility to decision-makers, allowing them to balance different factors depending on the specific situation.

C. Task Force Formed by the Maharashtra Government on Social Media Regulations for Minors

On 25 March 2025, the Maharashtra government announced a major policy shift. According to the state's 2022-23 economic survey, reported by the Times of India and the Special Inspector General of Police for the Prevention of Crime Against Women and Children, there were 16,836 crimes against children. The survey also pointed out that too much social media use is harming young people's mental and physical health.[18] NCBR data shows Maharashtra has the highest rate of cybercrimes against minors at 12.8%,[19] In response, the government has ordered a thorough, evidence-based investigation.

[17] Lis, Wojciech. "UN Convention on the Rights of the Child: Protection." (2024): 91-118. https://real.mtak.hu/228564/

[18] Nihar Behera et al., *Impact of Social Media Use on Physical, Mental, Social, and Emotional Health, Sleep Quality, Body Image, and Mood: Evidence from 21 Countries — A Systematic Literature Review with Narrative Synthesis*, 32 Int'l J. Behav. Med. (2025), https://doi.org/10.1007/s12529-025-10411-9.

[19] *Maharashtra Tops in Cybercrime Against Minors; Cases Up 196%*, Times of India (Jan. 3, 2022), https://timesofindia.indiatimes.com/city/mumbai/maharashtra-tops-in-cybercrime-against-minors-cases-up-196/articleshow/88655695.cms.

 [ISSN 2581-5369]

The task force will look into how minors use social media and how it affects their health, behaviour, learning, and social skills. It will also study how targeted digital ads impact young people. The group includes senior officials from the School Education Department, academics from the University of Mumbai, mental health experts from the Indian Psychiatric Society, NGO members, and representatives from social media companies. The panel will visit different regions and submit its findings in three months. The government will then use the report to create new policies.

This move drew significant attention during Maharashtra's budget session, especially after Karnataka became the first Indian state to officially regulate minors' access to social media. It marks a change in Indian federalism, with states taking a bigger role in digital rights and child protection, highlighting the shared responsibility of both Union and state governments for data protection, child welfare, and technology regulation.

III. ANALYSIS OF LEGAL AND REGULATORY FRAMEWORKS

In today's world, keeping children safe online is not about just one rule but a collaborative effort on each and everyone's part. This system attempts to balance key rights like protection, privacy, participation, and access to information in today's complex digital world. India has also enacted strong laws and policies to protect children from online risks such as cyberbullying, trafficking, and exploitation.

- **Constitutional Foundation**

India's strong commitment towards child protection commences with its constitutional framework. After becoming a part of the UN Convention on the Rights of the Child, provisions such as **Article 39(f)**[20] were given more importance to ensure that children grow up in a safe and healthy environment, which is free from exploitation and harm.

- **Legal Framework**

India has enacted several laws to address digital crimes against children. **The Information Technology Act, 2000** deals with cyber-crime related offences, while **the Protection of Children from Sexual Offences Act, 2012** provides strict safeguards against sexual crimes, including those occurring online. **National Commission for Protection of Child Rights** monitor and promote the protection of children's rights[21]. Additionally, specialized units and

[20] Article 39 of the UN Convention on the Rights of the Child makes it mandatory for the States to facilitate the physical/psychological recovery and social reintegration of child victims of neglect, abuse, exploitation, or armed conflict.

[21] Haag, A. C., & Bui, E. (2025). Beyond the algorithm: rethinking child protection in the digital age. *International Journal of Mental Health*, *54*(2), 152-153.

 [ISSN 2581-5369]

programmes have been established to detect, prevent, and respond effectively towards online exploitation of the children.

- **Multi-Dimensional Policy Approach**

India follows a comprehensive approach that is not limited to legal penalties. Policies like the National Cyber Security Policy focus on improving online safety, while the National Education Policy encourages awareness and responsible digital behaviour among children. Other measures aim towards providing support to parents and caregivers along with mental health assistance to children affected by online harm.

IV. ADAPTING TO TECHNOLOGICAL CHANGE

As digital technology is gaining a rapid growth in today's world, India is updating its laws and rules to keep up with the technology. New data protection laws are helping in maintaining the privacy of a child's personal information. At the same time, new features are being added such as parental controls to make the online space more secure. Overall, India is using a combined approach of laws, policies, institutions, and technology to make the online world safer for children while still allowing them to enjoy its benefits.

A. Judicial Pronouncements

In India, the judiciary plays a very proactive and imperative role especially in matters concerning the strengthening of this protection which is extended towards children as these are the future assets of our society. Courts have interpreted laws like the Information Technology Act, 2000 and the POCSO Act, 2012 in light of changing technologies and emerging online risks. Through such interpretations, they have not only helped in filling the legal gaps, but also immediate encouraged government action and made digital platforms more accountable[22]. As a result, the legal system has gradually become more effective in maintenance of children's rights in the digital space.

Indian courts through several important judgements have expanded the scope of fundamental rights under the Constitution to include protection in digital spaces. One of the most significant cases is ***'Justice K.S. Puttaswamy v. Union of India'***[23], where the Supreme Court held that the right to privacy is a fundamental right under **Article 21**, meaning that every individual including children, has the right to protect their personal data, even on digital platforms like social media,

https://www.tandfonline.com/doi/full/10.1080/00207411.2025.2493992

[22] Piyush Chaudhary, *Child Digital Safety Policy in India*, Int'l Inst. of SDGs & Pub. Pol'y Rsch., https://iisppr.org.in/child-digital-safety-policy-in-india/ (Mar. 31, 2026).

[23] *Justice K.S. Puttaswamy v. Union of India, AIR* 2017 SC 4161

apps, and websites. It further stated that any limits on this right must be lawful, have a clear purpose, be proportionate, and include appropriate safeguards.

The courts have also emphasised upon the shared responsibility of government institutions, internet platforms, and schools in ensuring safety of children online.

The madras high court in the case of **'S. Harish v. Inspector of Police,'**[24] initially were of the opinion that merely possessing child sexual abuse material (CSAM), without sharing it, was not punishable under the Protection of Children from Sexual offences Act (POCSO) or Information Technology Act (IT). However, this ruling was overturned by the supreme court in **'Just Rights for Children Alliance v. S. Harish,'**[25] where it was held that even the possession of such material can amount to a punishable offence, especially if it is not deleted or reported. The Court also recommended refraining from using the term "child pornography" and suggested the term "Child Sexual Exploitation and Abuse Material (CSEAM)" instead.

One of the landmark judgements related to digital media is **'Shreya Singhal v. Union of India,'**[26] in which the Supreme Court struck down **Section 66A of the IT Act, 2000**, holding it unconstitutional due to its vagueness and held that it violated the right to **freedom of speech under Article 19(1)(a).** While not directly related to the current topic of children, it underlined the need for clear and carefully curated laws to regulate online content, which is essential when dealing with issues like protecting children from online harm.

In **'Kamlesh Devi v. State of NCT of Delhi,'**[27] the Delhi High Court stressed upon the importance of protecting children from online grooming, also referred to as '**virtual touch**.' The Court denied bail to the accused, who had targeted a 16-year-old through social media platform, highlighting the seriousness of the issue of such persistent cases of digital offences.

B. Evaluating the Effectiveness of Intermediary Liability Under Section 79 of the IT Act in Addressing Child-targeted Algorithms

The concept of intermediary liability in India is governed by the Information Technology Act, 2000, which introduced the idea of 'safe harbour.' meaning that online platforms for instance, social media sites and search engines will not be held responsible for any content posted by users, as long as they follow certain rules. This protection is mainly provided under Section 79 of the Act. Earlier, intermediaries had the burden to prove that they were not aware of any such

[24] **S**. *Harish v. Inspector of Police,* 2024 SCC OnLine Mad HC (India)
[25] *Just Rights for Children Alliance v. S. Harish,* (2024) INSC 716 (S.C.).
[26] *Shreya Singhal v. Union of India,* AIR 2015 SC 1523
[27] *Kamlesh Devi v. State of NCT of Delhi,* 2024 SCC OnLine Del 3306

 [ISSN 2581-5369]

wrongdoing and had taken proper steps to prevent it.

This legislation was intended to support the growth of digital platforms and to protect them from severe liability, but may not meet the threshold to face new challenges, especially those related to algorithms that target children.

Algorithms are what decide what users see online. They suggest content based on a person's interests. For children, this is risky because such systems push content that keeps them engaged, which may sometimes be harmful, addictive, or inappropriate for their age. Unlike earlier systems, these algorithms now personalize content without any accountability on the part of the platform, which raises doubts about whether such platforms should still get legal protection under Section 79[28].

Under **Section 79(1)[29],** intermediaries are generally protected from liability for third-party content. However, this protection is not absolute. **Sections 79(2)[30] and 79(3)[31]** clearly state that this immunity applies only when the intermediary plays a passive role and does not actively participate in any illegal activity. If the intermediary is involved in unlawful actions or fails to act after being informed about harmful content, it can lose this protection. The law also introduced a "notice and takedown" system, in which intermediaries are promptly required to take down illegal content once they are notified.

When children come across harmful content like cyberbullying, online grooming, or dangerous trends through these systems, it is difficult to claim that platforms are only passive actors. Such claims create a gap, allowing platforms to avoid responsibility by relying on safe harbour protection.

The Information Technology Rules, 2021 attempt to resolve this issue by requiring platforms to follow certain responsibilities, such as removing illegal content and setting up complaint systems. However, there is remains a lack of transparency in the fulfilment of such responsibilities or limitations on how children's data is used for targeted content.

C. Legal Landscape before and after 2009 Amendment

Section 79, before the amendment of 2009, gave only limited protection to intermediaries. Platforms could avoid responsibility for any third-party content if they could sufficiently prove

[28] Tambiama Madiega, Reform of the EU Liability Regime for Online Intermediaries, EUR. PARL. RES. SERV. (2020), https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf (accessed Mar. 31, 2026).
[29] Information Technology Act § 79(1), No. 21 of 2000, India Code (2000)
[30] Information Technology Act § 79(2), No. 21 of 2000, India Code (2000)
[31] Information Technology Act § 79(3), No. 21 of 2000, India Code (2000)

 [ISSN 2581-5369]

that they were unaware of the offence being committed or had taken reasonable steps to prevent it. This protection also applied only to offences under the IT Act.

In the landmark ruling of **'Google India Pvt. Ltd. v. Vishakha Industries,'**[32] a defamatory post was shared on a Google Group, and was not removed even after being informed, In this matter the court held that since defamation was not covered under the IT Act at that time, so Google could not claim protection. This case showed that intermediary protection was quite limited before the amendment.

But, after the 2009 amendment, the scope of **Section 79** was broadened in its protection to intermediaries. Now Intermediaries are not held liable for third-party content under different laws, not just the IT Act. However, such protection can be revoked if they fail to remove illegal content after receiving proper notice.

Another frequently raised question was whether platforms should check all content themselves. This was clarified in Shreya Singhal case, where the Supreme Court stated that intermediaries are not required to monitor all content. They only need to act when they receive a court order or official notice.

Similarly, in **'MySpace Inc. v. Super Cassettes India Ltd.,**'[33] the Delhi High court held that screening all content was impractical and would have a negative impact on freedom of speech and privacy.

D. Data Privacy, Consent and the Rights of Children in the Digital Age: An Analysis Under the DPDP Act, 2023

The internet is now a staple in children's lives, making them both important and vulnerable online. Unlike adults, children are not capable of fully grasping the risks of sharing personal information or other communication with strangers, highlighting the need for legal protection. The Digital Personal Data Protection Act, 2023, is the primary law for this, but there are still questions about whether its rules are enough.

Section 2(f) of the act defines a child as any individual under eighteen years of age, establishing a stricter threshold than most international standards. The United States' Children's Online Privacy Protection Act applies only to children under thirteen.[34]

The DPDP Act calls the platforms, apps, and services that collect personal data 'data fiduciaries.

[32] *Google India Pvt. Ltd. v. Vishakha Industries,* (2020) 4 SCC 162
[33] *MySpace Inc. v. Super Cassettes India Ltd.,* 2016 SCC OnLine Del 6382
[34] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), ch. 1, https://dpdpact2023.com/chapter-1

 [ISSN 2581-5369]

These data fiduciaries must safeguard the data. Section 9(1) of the Act requires data fiduciaries to obtain 'verifiable parental consent' before processing any data from a child user. If they do not comply, they may face penalties of up to Rupees 200 crore.[35]

The Problem with Verifiable Parental Consent

Although the Act requires parental consent, implementing it is difficult. Platforms must confirm whether a user is a child, verify the guardian relationship, and record the user's identity when obtaining consent. If these steps are not followed, the consent is invalid.[36]

The Act does not explain exactly how platforms should meet these requirements and leaves the details for future rules. The government recommended using Digi Locker for this purpose, but that too came with its share of concerns. Often, more information is collected than is needed for consent, creating permanent digital records and increasing privacy risks.[37].

Age Verification and the Right to Privacy

There are several methods of verifying age, each with their own pros and cons. Self-verification is easy but can be bypassed. Biometric methods, such as facial age checks, are more accurate but cannot always confirm the exact age required by the DPDP Act. AI-based profiling can reinforce social biases and hurt privacy. Government ID checks are the most accurate, but also raise privacy concerns. In the United States, enforcing COPPA has been difficult: high costs prevent platforms from offering child-safe services, and penalties have not changed platform behaviour much.[38]

The European Union's GDPR adopts a flexible framework, where the member states set the age for digital consent between 13 and 16 years, and platforms are mandated to make 'reasonable efforts' to verify consent[39]. They are developing an age verification system called EU Consent, which allows users to verify their identity once and use that verification across platforms without revealing unnecessary personal information[40].

---

[35] Pankaj Doval, *Data Protection Bill: Govt Plans Penalty of Up to Rs 500 Crore for Data Breach*, Times of India (Nov. 19, 2022), https://timesofindia.indiatimes.com/india/govt-plans-penalty-of-up-to-rs500cr-for-data-breach/articleshow/95613899.cms

[36] *DPDP Rule 10: A Practical Guide for Child Data Protection*, Privacy Global (2025), https://www.privacyglobal.org/blog/dpdp-rule-10-consent-for-childrens-data-processing.

[37] Aakash Burman, *Understanding India's New Data Protection Law*, Carnegie Endowment for Int'l Peace (Oct. 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law

[38] *COPPA Safe Harbor Program*, Fed. Trade Comm'n, https://www.ftc.gov/enforcement/coppa-safe-harbor-program (last visited Mar. 31, 2026).

[39] *Article 8: Conditions Applicable to Child's Consent in Relation to Information Society Services*, GDPR.eu (2016), https://gdpr.eu/article-8-childs-consent/.

[40] *EU Targets Snapchat over Child Safety and Accuses Porn Sites of Failing to Block Minors*, AP News (Mar. 27, 2026), https://apnews.com/article/8a53ec642c7a8f711988f141aa6ff6ec.

 [ISSN 2581-5369]

The United Kingdom's Age-appropriate Design Code (Children's Code) has prompted platforms to implement default privacy settings for children, restrict adult-to-minor messaging, and disable certain features for users under 18. The Online Safety Act further reinforces these requirements.[41]

The DPDP Act is an important move for children's digital rights in India. To make the most of it, India needs clear, enforceable rules, flexible age-verification methods that cover all children, and lessons from international best practices. The most important factor in any decision should be the safety and dignity of the children.

V. CHALLENGES IN IMPLEMENTATION

Although the intention behind the proposal of these regulations is genuine concern for mental health, safety, and well-being of our youth, the effectiveness and enforcement of the same is faced with significant practical, constitutional, and socio-economic challenges. Before any such regulations are passed the complexities of implementation should be studied to determine whether the regulations will achieve their intended goals.

Digital exclusion

A major challenge in implementing social media bans for adolescents is the risk of widening of current digital inequalities. Adolescents in rural and low-income households often rely on social media for educational content, scholarship information, peer learning, and career guidance. For students in under-resourced schools or with limited access to libraries or coaching centres, social media can be essential. The legal and policy challenge is to design a regulatory framework that protects vulnerable children from online harm without simultaneously excluding them from digital opportunities essential to educational and career advancement.

Enforcement of Age Verification

Setting age-based limits on social media is technically and administratively challenging. It is hard to verify age across many platforms and millions of users. Right now, no age verification system under the DPDP Act, 2023, meets the needed standards for accuracy, coverage, and privacy. Currently, as stated by the French data regulator CNIL, no existing solution, including self-verification or biometric and AI-based facial recognition tools, meets the threefold standard of sufficient and reliable verification, complete population coverage and adequate privacy protection. Any framework that mandates age verification must resolve these technical

[41] *Keeping Children Safe Online: Changes to the Online Safety Act Explained*, Gov.UK (Aug. 1, 2025), https://www.gov.uk/government/news/keeping-children-safe-online-changes-to-the-online-safety-act-explained

obstacles.

Mental Health Paradox

One of main and most commonly acknowledged reason for these regulations is to protect the mental health of the youth which is adversely affected by unregulated social media use. However, strict regulation also comes with challenges, especially the absence of the positive side of social media which helps children connect and socialize with their contemporaries and get emotional support when they have nowhere else to get it.

India's mental health system is not well developed, and there is still stigma around seeking professional help, where some families even refuse to acknowledge a mental health struggle or problem. Sometimes, social media can act as an easy way to connect with friends, find information, and get support. Therefore, any suggested interventions should be paired with alternative mental health support systems, rather than relying solely on regulation as the solution to the problem. Simply banning or regulating social media, which indeed does have an impact on mental health is not enough, when there are people who rely on it for survival have nowhere else to go.

Constitutional Challenges

Adolescence is a time for exploring one's identity, self-expression, morals and values. Lately, social media has become a place where children choose to embark on their self- exploration journey, to express their views and connect with like-minded individuals. This can serve as a helpful avenue for youngsters to navigate their personalities as it makes interacting instant and very accessible.

Absolute regulation of social media for children raises questions of violation of fundamental rights under Article 19(1)(a) and Article 21 of the Constitution. Any restriction on the rights mentioned under these sections must be proportional and reasonable. A blanket ban that fails to distinguish between harmful and beneficial uses of social media is likely to face serious constitutional challenges.

Digital Literacy

Digital literacy is crucial in a person's education and professional life, and using undeniably social media helps build these skills. Learning to navigate safely online, check whether information is trustworthy, and spot risks is best done through guided, regulated use of digital spaces. Good implementation should focus on making digital participation safe, informed, and empowering for children, instead of shutting them out completely.

 [ISSN 2581-5369]

VI. SUGGESTIONS

- **Evolution of a tiered, risk-based framework**: The government should calibrate restrictions to the nature and level of risk associated with specific platforms and content categories. Platforms offering content legally prohibited to minors, such as adult content and gambling, should face a harsher age verification requirement. General social media platforms should have age-verification mechanisms in place, combined with a robust default safety setting. This approach, based on the United Kingdom's Age-appropriate Design Code, protects children from serious harm while preserving access to the educational, social, and developmental benefits of the digital age.
- **Platform responsibility:** The safe harbour rule in Section 79 of the IT Act should be amended to impose active duties on platforms, not just passive ones. Platforms must be required to publish regular impact assessments for children's usage and to make sure their recommendation systems do not show harmful or age-restricted content to children. If platforms do not meet these requirements, they should face real penalties to encourage better re-design. Unless there is no accountability on the part of the platforms, the regulations alone cannot bear the brunt of child protection. The platforms should also remain transparent on the data usage and storage, submitting reports to the Data Protection Board and making them public.
- **Building age-verification systems**: A group including technology experts, child rights groups, privacy experts, civil society, and children should be constituted by the government to develop a code of practice for age authentication. This system can leverage existing tools such as Digi Locker and the Account Aggregator framework. These systems must be fair, protect privacy and work efficiently and accurately.
- **Digital Literacy:** A long-term national programme should be established to educate adolescents on the ways of navigating the internet safely, verify information, understand their data rights, and report online harm. This should be done through schools, community centres, and online platforms. Parents and teachers should also be made aware of this information so they can guide children well.
- **Establishment of an independent Children's Digital Rights Commissioner:** Modelled after the UK's Children's Commissioner or Australia's eSafety Commissioner, India should also set up an independent body to protect and promote children's rights online. This group should be able to investigate complaints, do research, give advice to platforms and regulators, and make binding recommendations to the government. The group should consist

 [ISSN 2581-5369]

of child rights experts, mental health professionals, technologists, educators, and civil society members who work with children.

A collaborative effort among lawmakers, regulators, platforms, educators, parents, civil society, and children can lead to the formation of a safer digital environment for our future. The groundwork has been laid in the form of DPDP Act, debates in Parliament about a social media ban, and involvement from courts. Now we must treat this matter with urgency and ensure a safer world for our youth.

VII. CONCLUSION

The regulation of children's social media access raises significant questions about rights, state power, responsibilities of platforms and the meaning of childhood in a digital world. Evidence clearly shows that excessive and unregulated social media use impacts the mental health of its users, causes addictions, exposes children to harmful content and may lead to the exploitation of minors' data. [42] The Indian Psychiatric Society has documented a significant rise in mental health disorders in minors, and the Economic Survey by the Union Finance Ministry highlights this as a national concern[43]. The state has the constitutional authority and the moral responsibility to respond to this crisis.

However, any response must be evidence-based and proportionate. A blanket ban, while well-intentioned, risks deepening the digital divide, the migration of children to unregulated platforms, and raises constitutional questions under Articles 19 and 21 of the Indian Constitution. Comparative jurisdictions such as the United States, Australia, and France, too, have not been able to develop a system that fully protects children online while preserving their right to digital participation.[44] Thus, the fight to create safe digital environments for children still continues.

*****

[42] Ibid

[43] *Digital Addiction Emerging as Major Concern in Children and Youth: Economic Survey 2025–26*, NDTV (Jan. 29, 2026), https://www.ndtv.com/health/govt-flags-growing-digital-addiction-mental-health-crisis-in-children-youth-10906029.

[44] Helen Stalford & Laura Lundy, *Whose Business?: Protecting Children's Rights in the Online Environment*, 33 Int'l J. Child. Rts. 1 (2025).

 [ISSN 2581-5369]