Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Growing up Online: Safeguarding Children's Rights in Digital Playgrounds

Sumit Pandey[a]

[a]University of Delhi, New Delhi, India

Received 30 June 2025; *Accepted* 30 July 2025; *Published* 04 August 2025

In the digital era, children's use of the Internet for study, recreation, and social interaction is steadily increasing. This connectedness has many advantages, but it also creates problems that disproportionately harm children owing to their fragility and ignorance. Cyberbullying, Online Gaming, Data abuse, AI-generated deepfakes, and exposure to harmful content are just some examples of threats that demand urgent legal, technical, and social remedies. This article critically analyses the global and Indian frameworks for children's rights and safeguards in the digital world, focusing on instruments such as the UNCRC, the Information Technology Act 2000, the Protection of Children from Sexual Offences 2012, and the Digital Personal Data Protection Act 2023. It also examines landmark case laws, identifies policy gaps, and addresses current issues like AI and misinformation. Adopting a child-centric view, this article highlights the need for a balanced approach that protects children's right to access information and express themselves online, while preserving their safety, privacy, and dignity. Achieving this requires systematic measures encompassing legal protections, ethical digital practices, public awareness, and education.

Keywords: *children, privacy, child's safety, artificial intelligence, grooming.*

INTRODUCTION

The 21st century has witnessed an unprecedented digital revolution, which has transformed people's way of life, learning, and communication. Children, whose early years are increasingly influenced by technology, are among those most impacted by this change. Through online classrooms, online games, video-sharing platforms, and learning aids driven by Artificial Intelligence, children today are immersed in a virtual realm that is both pervasive and perilous.

With the advancement of technology, children have many possibilities at their fingertips. Instantaneous information, worldwide peer connections, and the opportunity to develop employable skills are all within their reach. Cyberbullying, identity theft, exploitation, misinformation, and psychological discomfort due to excessive screen time or algorithm-driven content are some examples of risks that may affect children using the same tools that empower them. The line between benefits and risks is very thin for a child who cannot completely understand the consequences of their online activity.[1]

The issue of children's internet safety has become more prominent on a global scale. Child welfare organisations and UNICEF have found that internet abuse and exploitation are on the rise. The COVID-19 pandemic further accelerated the children's screen dependency and vulnerability, shifting their social and educational environment into the online domain. This has made the protection of children in cyberspace an important matter of public policy, law, and child rights.

LAW AND CHILD RIGHTS

In India, internet users are growing rapidly, which generates unique challenges. Every day, millions of youngsters use the internet; consequently, the country's legal framework has evolved to accommodate these new realities. The right to privacy and digital well-being is implicitly included in the right to life & dignity guaranteed under Article 21 of the

[1] Anupam Sharma, 'Globalization and its impact on cybercrime: A case study of Indian police administration' (2017) 56(2) Indian Journal of Public Administration <http://doi.org/10.1177/0019556120100203> accessed 11 May 2025

Constitution. However, there are significant protection gaps in current laws, which struggle to keep pace with the speed of technological change.[2]

This research article aims to fill these gaps by examining the rights & protection that children have in the digital era. It reviews current laws, evaluates emerging cyber threats, and discusses how the courts and government are responding to them. By adopting a child-first approach, this article underscores the importance of building a more robust and future-ready system that empowers and protects them in equal measure.

Ultimately, the protection of children in the digital era is more of a social need than a technological or legal one. When a country takes measures to ensure the safety of its younger users, it demonstrates its commitment to democratic values, human dignity, and inclusive development. Innovation must co-exist with integrity; freedom with responsibility, and access with accountability if we are to progress.

LEGAL FOUNDATION OF CHILDREN'S RIGHTS IN THE DIGITAL SPHERE

International Framework –

United Nations Convention on the Rights of the Child (UNCRC):[3] The cornerstone of children's rights at the international level is the UNCRC, adopted in 1989. While it predates the digital revolution, its principles remain highly relevant in the digital age. Articles 13, 16, and 17 of UNCRC[4] directly pertain to a child's freedom of expression, protection from arbitrary interference with privacy, and access to appropriate information through mass media.

General Comment No. 25[5] was presented in 2021, specifically addresses children's rights in the digital environment. This document emphasises the need to safeguard children's rights online as rigorously as offline. It calls for the creation of laws, policies, and an environment that provides fair access to digital resources, protects users from online risks, and encourages digital literacy and safety.

[2] The Constitution of India 1950
[3] United Convention on Rights of Child 1989
[4] United Convention on Rights of Child 1989, arts 13, 16 and 17
[5] General Comment No. 25 on Children's Rights in Relation to Digital Environment 2021

Sustainable Development Goals[6] **-**

The Sustainable Development Goals (SDGs) were adopted by the United Nations in 2015, aiming to ensure a better and more sustainable future for all by 2030. Several SDG goals relate to protecting children in the digital sphere:

SDG 3 - Good Health and Well-being: Promote mental health by preventing online bullying, screen addiction, and social media pressure.

SDG 4 - Quality Education: Ensure all children have equal access to quality online learning platforms and digital tools

SDG 16 - Peace, Justice, and Strong Institutions: Protect children from abuse, exploitation, trafficking, and violence against them in the real and digital sphere.

SDG 17 - Partnership for Goals: Government, tech companies, Schools, and families must work together to make the internet safer and fair for children.

ECOSOC Resolution 2011/33:[7] Economic and Social Council Resolution 2011/33 on Prevention, Protection and International Cooperation against the Use of New Information Technologies to Abuse and/or Exploit Children is a resolution issued by the United Nations Economic and Social Council. The resolution initiated a study on how this information and electronic technologies impact crimes against children.

The Rio de Janeiro Duration:[8] The Third World Congress against Children's Exploitation was held in Rio De Janeiro, Brazil, in the year 2008. The declaration aimed to take effective steps to combat the sexual exploitation of children. It focused on the causes and reasons behind the sexual exploitation of children and discussed strong, comprehensive strategies, such as Millennium Development Goal 21, to prevent and combat this crime by eradicating extreme poverty and hunger.

---

[6] 'Transforming our world: the 2030 Agenda for Sustainable Development' (*United Nations*) <https://sdgs.un.org/2030agenda> accessed 02 June 2025

[7] ECOSCO Resolution on prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children 2011, res 33

[8] 'The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents, Document from the III World Congress against Sexual Exploitation of Children and Adolescents' (*World Congress Against Exploitation of Children and Adolescents*) <https://www.mofa.go.jp/policy/human/child/congress0811-d.pdf> accessed 02 June 2025

CONSTITUTIONAL & LEGAL PROVISIONS IN THE INDIAN CONTEXT

The Constitution of India –

Art 21:[9] Guarantees the Right to Life & Personal Liberty, which courts have interpreted to include the right to privacy, dignity, education, and digital safety.

Art 39(e) & (f): The Directive Principles of State Policy direct the State to ensure that children are not abused & that their childhood is protected.[10]

Art 45: The State shall endeavour to provide, within ten years from the commencement of this Constitution, for free and compulsory education for all children until they complete the age of fourteen years.[11]

IT Act:[12] The IT Act is India's primary cyber law. Some sections are child-specific: Section 66E[13] penalises violation of privacy through capturing, publishing, or transmitting private images without consent; Section 67B[14] specifically criminalises the publishing, browsing, or downloading of child sexual abuse material; and Section 69A[15] grants the government power to block content harmful to the public, including children.

POCSO:[16] This Act comprehensively addresses the sexual offences against children, including those facilitated through digital means. Sections 11 & 12 address sexual harassment, which includes sending lewd messages or engaging in online sexual communication.[17] Section 15[18] provides for the penalisation of the storage, possession, or distribution of child sexual abuse material.

JJ Act:[19] While primarily a welfare legislation, it mandates the State to protect children from abuse, neglect, and exploitation in all settings, including online.

[9] Constitution of India 1950, art 21
[10] Constitution of India 1950, arts 39(e) and (f)
[11] Constitution of India 1950, art 45
[12] Information Technology Act 2000
[13] Information Technology Act 2000, s 66E
[14] Information Technology Act 2000, s 67B
[15] Information Technology Act 2000, s 69A
[16] Protection of Children from Sexual Offences 2012
[17] Protection of Children from Sexual Offences 2012, s 11 and 12
[18] Protection of Children from Sexual Offences 2012, s 15
[19] Juvenile Justice (Care and Protection of Children) Act 2015

The DPDP Act:[20] The recent legislation represents a crucial development in the digital rights landscape. It introduces the concept of 'verifiable parental consent' for processing data of minors.

Key Highlights: No tracking, targeted advertisement, or data monetisation is allowed for users under 18 years of age, without parental consent. Companies handling children's data must adopt higher standards of security.

SECTOR-SPECIFIC GUIDELINES & REGULATIONS

National Education Policy 2020: The NEP acknowledges the importance of integrating digital tools in education and calls for safety & security training, digital citizenship education, and child-friendly tech policies in schools.

NCERT guidelines on Cyber safety 2021: These guidelines suggest age-specific recommendations for schools and parents, covering: digital etiquette, cyberbullying awareness, protection from online predators, and responsible social media use.

Regulation:[21] Platforms like YouTube, Meta, Prime, and Netflix have introduced restricted modes, content rating systems, and child-specific applications. However, many of these remain optional and depend on parental awareness & control.

EMERGING THREATS TO CHILDREN IN THE DIGITAL AGE

Children in today's rapidly evolving digital world face several dangers when they go online, some of which are obvious, while others are more subtle but equally damaging.[22] By increasingly using the internet for education, communication, and entertainment, children also become vulnerable to dangers that compromise their safety, privacy, emotional well-being, and overall development. The following are emerging threats in detail:[23]

Online Sexual Exploitation and Abuse: One of the gravest threats faced by children online is sexual exploitation and abuse. Sometimes, over long periods, criminals groom children by

[20] Digital Personal Data Protection Act 2023
[21] Advisory on adherence of Indian Laws and the Code of Ethics prescribed under the Information Technology (Intermediary Guidelines and Digital Media, Ethics Code) Rule 2021
[22] Igor Bernik, *Cybercrime & Cyberwarfare* (Wiley 2014)
[23] Anupreet Kaur Mokha, 'A Study on Awareness of Cyber Crime and Security' (2017) 8(9) Research Journal of Humanities and Social Sciences <http://dx.doi.org/10.5958/2321-5828.2017.00067.5> accessed 01 June 2025

gaining their confidence via social media, messaging applications, and online gaming platforms.

Forms of Exploitation –

Child Sexual Abuse Material (CSAM): Explicit images or videos of a child being shared or sold.[24]

Live-streamed Abuse: It becomes more difficult to identify and prosecute offenders when they live-stream abuse.

Grooming: Offenders often create fake profiles and lure children into inappropriate relationships, sometimes leading to blackmail (sextortion).[25]

Cyberbullying and Online Harassment: Cyberbullying has become increasingly common among children and teens. It includes sending threatening or abusive messages, posting embarrassing photos or videos, and spreading rumours on social media. Extreme cases of cyberbullying may result in suicidal thoughts, despair, social withdrawal, and anxiety. Some platforms lack real-time monitoring and child-friendly reporting systems, making it more difficult for victims to seek aid.[26]

Privacy Invasion and Data Exploitation: Children often use applications and platforms that collect personal data, sometimes without their knowledge or that of their parents. Key concerns include: Surveillance-based advertising where children's online behaviour is tracked and used to create marketing profiles, violating their privacy; lack of informed consent, as children may not knowwhat they are agreeing to when apps request permissions; data breaches, where educational platforms or gaming apps get hacked and sensitive data related to children can be leaked or sold on the dark web; exposure to inappropriate content, where children may encounter violent or graphic media, pornographic content, self-harm or suicide-related discussions (e.g., Blue Whale Challenge), misinformation and conspiracy theories, etc. Algorithms on platforms like YouTube or TikTok often auto-suggest such

[24] Sana Ali et al., 'Child Sexual Abuse and the Internet—A Systematic Review' (2021) 4(1) Human Arenas <https://link.springer.com/article/10.1007/s42087-021-00228-9> accessed 01 June 2025
[25] Konstanze Schoeps et al., 'Risk factor for being a victim of online grooming in adolescents' (2020) 32(1) Psicothema <https://doi.org/10.7334/psicothema2019.179> accessed 01 June 2025
[26] Swarndeep Singh et al., 'Quality of online news media reports of child sexual abuse in India' (2022) 31(2) Industrial Psychiatry Journal <https://doi.org/10.4103/ipj.ipj_238_21> accessed 01 June 2025

content, creating echo chambers that worsen mental health outcomes. Parental controls exist, but are often complex or easily bypassed.

Radicalisation and Extremist Propaganda: Some children are targeted by extremist groups online to influence their thinking and behaviour. These groups use encrypted platforms and chat rooms, memes and gamified propaganda, false historical narratives and religious extremism. This is especially dangerous for vulnerable or isolated children, as radical content may appear alongside innocuous videos or games.[27]

Gaming Addiction and Online Gambling: With the rise of mobile gaming, children are increasingly spending long hours on apps like PUBG, Free Fire, or Call of Duty. Risks include poor academic performance and disturbed sleep due to gaming addiction. In-game purchases can lead to financial exploitation and exposure to gambling mechanics (loot boxes, betting apps) disguised as gaming. India currently lacks a national policy regulating children's online gaming habits, although several states have proposed age-based limits.

Deepfakes and Digital Manipulation: Deepfake technology, powered by AI, allows malicious actors to create highly realistic fake videos or voice recordings of children, which can be used for sextortion, bullying, false accusations, manipulated consent videos, and similar abuses

Misinformation and Algorithmic Bias: Children often rely on social media or unverified sources for information. Misinformation campaigns can distort their worldview, promote hatred or discrimination encourage unhealthy behaviour (fake health cures, diet trends, etc.) Even algorithms have the potential to show biased material, which may amplify prejudices and suppress diversity, for example, biased image suggestions, YouTube recommendations, and content visibility.[28]

Online Radical Gender or Racial Narratives: Teenagers are often exposed to extreme gender or racial narratives online. Examples include Incels (involuntary celibates) communities promoting misogyny, hate groups promoting racist ideologies, and toxic beauty standards

[27] Maria Bada and Jason R.C. Nurse, 'The social & psychological impact of cyber-attack' in Vladlena Benson and John Mcalaney (eds), *Emerging Cyber Threats and Cognitive Vulnerabilities* (Academic Press 2020)
[28] Donghee Shin, *Artificial Misinformation: Exploring Human-Algorithm Interaction Online* (1st edn, Palgrave Macmillan 2024)

that marginalise certain races or ethnicities. Without the ability to critically evaluate the content, children are especially vulnerable to adopting harmful beliefs.[29]

Psychological and Developmental Impact: The cumulative effect of these threats manifests in attention deficiencies and low cognitive abilities, poor social attraction due to over-dependence on virtual attraction, anxiety, depression, and identity confusion. Sleep disorders & behavioural changes are common. Overuse of screens also leads to physical issues such as vision problems, obesity, and posture-related complications.[30]

Parental and Institutional Challenges: Many parents are unaware of their children's online activities. Key obstacles include limited digital literacy among guardians, insufficient digital safety education in schools**,** over-reliance on paid parental control software, and a trust deficit between children and caretakers. Unfortunately, many schools lack cyber counsellors and secure reporting mechanisms, making it harder for children to report online harassment.

Institutional and Civil Society Initiatives: Protecting children in India from online harm is a shared responsibility across various sectors of society. To create a safe online space, public agencies, nonprofits, and even for-profit businesses are collaborating on awareness and protection programs.

Government Initiatives: The Indian government has introduced various programs and policies aimed at addressing online threats and educating children about digital safety:

- **National Commission for Protection of Child Rights (NCPCR):** The NCPCR plays a crucial role in developing cyber safety standards for children. A joint advisory with MeitY lays out steps that parents, schools, and social media companies should take to combat child abuse on these platforms.
- **Cybercrime Prevention against Women and Children (CCPWC) Scheme:** Launched by the Ministry of Home Affairs, this scheme assists states and UTs in enhancing their cybercrime units and provides funding for awareness programs and capacity building initiatives.

[29] Priyamvada Gopal, *Literary Radicalism in India: Gender, Nation and the Transition to Independence* (1st edn, Routledge 2005)
[30] Bada (n 27)

- **Digital India Programmed:** Though not child-specific, it includes digital literacy programs like PMGDISHA (Pradhan Mantri Gramin Digital Saksharta Abhiyan), which can be used to educate families and children on basic digital hygiene.[31]
- **Cyber Crime Reporting Portal (https://cybercrime.gov.in):** This portal provides a platform to anyone (including children and parents) to report offences like cyberbullying, grooming, and exploitation.[32]
- **NGO and Civil Society Efforts:** There is a critical shortage of resources to address children's digital safety, but several non-governmental organisations (NGOs) in India actively work to fill this void through education and protection.
- **Cyber Peace Foundation:** Serving children in underserved and rural regions, this non-governmental organisation (NGO) collaborates with the Indian government and UNICEF to provide workshops on digital literacy. It's the Cyber Peace Club program promotes in-school collaborative learning on topics such as cyberbullying, online grooming, and disinformation.
- **Save the Children India:** This organisation runs multiple projects focused on online safety awareness, particularly targeting adolescent girls who are vulnerable to online exploitation and cyberstalking.
- **Bachpan Bachao Andolan:** While historically focused on ending the exploitation and trafficking of children, this group has recently shifted attention to how the internet and digital communication affect children's rights and protection.
- **Children India Foundation (1098):** Primarily, a women's protection helpline, it also handles cases related to online abuse and exploitation of children, providing immediate intervention and referrals.

Public-Private Partnerships and EdTech Platforms –

Tech companies and social media platforms also play a vital role in child safety. In recent years, partnerships between governments, civil society, and private companies have been encouraging:

[31] Amit Tiwari et al., 'DIGITAL INDIA INITIATIVES: AN EDUCATIONAL PANORAMA' (Conference: DIGITAL INDIA INITIATIVES: AN EDUCATIONAL PANORAMA 2017)
[32] Ritu Chhabra Dr. Sushil Kumar Singh, 'RIGHTS OF CHILDREN IN CYBER WORLD INDIAN PERSPECTIVE' (2020) 43(4) Sambodhi

- **Meta (Facebook, Instagram):** Meta has launched a Parents' Guide for Instagram in India, in partnership with organisations such as Aarambh India Initiative. It educates parents and teens about safe usage.
- **Google's Be Internet Awesome Campaign:** This includes interactive games and classroom materials that help children learn how to identify scams, create strong passwords, and interact respectfully online.
- **EdTech Platforms:** Companies like BYJU, Vedantu, and others are increasingly embedding content moderation and child-safety tools, although a standardised child-safety policy across platforms is still lacking.

School-Based Initiatives: Recognising schools as key stakeholders, the government has introduced cyber safety modules under the Digital India initiative. Programs like Cyber Surakshit Bharat and Information Security Education & Awareness (ISEA) have been launched for students and teachers, alongside CBSE advisories on digital etiquette and the safe use of social media.

Role of Intermediaries and Tech Platforms: Under the IT Rules (2021), online platforms are required to remove objectionable content within 24 hours of a complaint, deploy AI-based content moderation and appoint grievance officers for faster redressal.

Judicial Interventions: The Indian judiciary has played an active role in expanding digital protections. Through various judgments, Courts protected children's rights in the digital sphere & reshaped the digital environment.

CASE LAWS

Avnish Bajaj v State:[33] It is the first significant case addressing intermediary liability for content concerning children. In this case, the court emphasised the responsibility of intermediaries in the distribution of obscene material involving minors.

[33] *Avnish Bajaj* v *State* (2005) 79 DRJ 576

Shreya Singhal v Union of India:[34] This landmark ruling declared Section 66A of the Information Technology Act 2000, unconstitutional and laid the foundation for protecting minors from vague digital criminal law.

In Re: Prajwala Letter Case (2017):[35] This case is related to the circulation of rape & child pornography videos online. The Hon'ble Court issued directions to the government and tech companies to develop mechanisms for removing child sexual abuse material.

In Re: Children in Street Situation (2022): In this case Hon'ble Court recognised the need for safe digital access, identity-linked entitlements, and online education safeguards.

Facebook India Online Service Pvt. Ltd. v Union of India (pending): This case underscores the balance between privacy and safety, especially in protecting children from online sexual exploitation, cyberbullying, and grooming. It highlighted the accountability of platforms in removing & preventing the spread of CSAM.

Just Rights for Children Alliance v S. Harish (2024):[36] This case emphasised the urgent need to protect children from online abuse and exploitation. The court called for robust digital safeguards, holding platforms accountable, and ensuring children's rights to safety, dignity, and privacy in the digital environment.

INTERNATIONAL PERSPECTIVES AND BEST PRACTICES

India's efforts should be benchmarked against global standards to build an effective framework for protecting children in the digital age.

European Union's General Data Protection Regulation (GDPR):[37] The GDPR imposes strict rules on processing children's data, requiring parental consent for users under 16 and ensuring that data is processed in a manner that protects the child's best interests. Similarly, the UK's Age-appropriate design code mandates privacy-by-default settings for minors. While India's Digital Personal Data Protection Act 2023 provides comparable safeguards, it does not yet mandate.

---

[34] *Shreya Singhal* v *Union* of *India* AIR 2015 SC 1523
[35] *In Re: Prajwala Letter Case* SMW (Crl) No 03/2015
[36] *Just Rights for Children Alliance v S. Harish* Crl App Nos 2161-2162/2024
[37] General Data Protection Regulation 2016

United States: Children's Online Privacy Protection Act (COPPA)[38] To protect children's privacy, websites and online services must have their parents' verified permission before collecting personal information from children under the age of 13. COPPA Law has been criticised for failing to adapt to new types of data collection via AI and IoT devices, yet it is still a fundamental regulation in the US that protects children. India does not yet have a dedicated online privacy law for children, relying instead on broader frameworks that offer limited enforcement.

Australia: Online Safety Act 2021 and Amendment 2024:[39] This law empowers the e-Safety Commissioner to make an order to remove harmful content, including cyberbullying and image-based abuse, to offer a reporting tool for youth experiencing online harm and to regulate online platforms with a safety code of conduct. It establishes a One-stop grievance redressal, which is combined with strong enforcement and platform accountability. The idea of a separate agency responsible for children's internet safety might help Indian organisations consolidate their fragmented governance structures.

South Korea: Digital Well-being and Screen Time Regulation:[40] South Korea adopts a techno-cultural approach. By law, smartphones sold to minors must have parental controls installed to avoid smartphone addiction. The government-funded digital detox camps and cyber wellness education. This approach balances protection with mental health promotion and digital literacy. In India, similar behavioural support programs in schools could reduce the overuse and online gaming addiction.

Global Guidelines: UNICEF and ITU Frameworks:[41] UNICEF's *Children's Rights in the Digital Age* Report and the International Telecommunication Union (ITU) guidelines serve as global references, highlighting the importance of children's involvement in the process of development of digital regulations, strongly encourage governments to prioritise equitable access and digital inclusion and call for measures to prevent algorithmic bias. India has been

[38] Children's Online Privacy Protection Act 1998
[39] Online Safety Amendment (Social Media Minimum Age) Act 2024
[40] Kyung Soo Woo et al., 'Mental Health, Smartphone Use Type, and Screen Time Among Adolescents in South Korea' (2021) 14 Psychology Research and Behavior Management <https://doi.org/10.2147/prbm.s324235> accessed 01 June 2025
[41] 'Guidelines for industry on Child Online Protection 2020' (*ITU Publications*) <https://www.unicef.org/media/90796/file/ITU-COP-guidelines%20for%20industry-2020.pdf> accessed 13 May 2025

an active partner in these forums, but it can do more to incorporate these principles into domestic policy and legislation.

Civil Society and NGO Innovations Worldwide: Internationally, NGOs and private players are shaping child-friendly digital ecosystems. The 5 Rights Foundation (UK) advocates for child-centric internet design., Common Sense Media (US) offers reviews of digital content and privacy ratings for parents and schools, and Child Helpline International supports cross-border emergency assistance for cases of digital child abuse**. Takeaway for India**: There is potential for stronger public-private partnerships to create localised tools and platforms that meet India's linguistic and cultural diversity

Technological Interventions in Other Countries: Various countries are using AI and data science to track online harm. Germany's NetzDG law uses automation and dedicated teams to remove illegal content quickly, Singapore employs AI to detect grooming behaviour on children's gaming platforms, and New Zealand collaborates with tech firms to use image hashing to fight child sexual abuse material (CSAM). India's Opportunity to invest in ethical AI systems for content moderation, real-time threat detection, and localised response systems in Indian languages.

POLICY GAPS, FUTURE CHALLENGES, AND THE ROAD AHEAD

Despite notable legislative advances, India's digital child protection framework remains fragmented and under-equipped to tackle the pace and complexity of the evolving digital environment. This section examines policy gaps, potential problems, and proposed reform strategies in detail.

Key Policy Gaps in India's Current Framework –

1. Lack of a Dedicated Law for Online Child Safety: While laws such as the IT Act, POCSO Act, and Data Protection Act provide some protective provisions, none specifically deal with children's digital rights. This leads to ambiguities in enforcement (e.g., age verification for apps), overlaps and contradictions between ministries and law enforcement bodies, and limited child-specific redressal mechanisms.

2. Inadequate Age-Verification Standards: India lacks mandatory, standardised age-verification tools across platforms. As a result, children easily access age-inappropriate

content (e.g., violent games, adult media), and apps collect sensitive data from minors without valid consent.

3. No Regulatory Body for Child Digital Welfare: Unlike Australia's e-Safety Commissioner, India has no central authority focused solely on the digital well-being of children. NCPCR's role is broad and under-resourced.

4. Poor Implementation of School-Based Digital Literacy: Most government and private school curricula lack education on digital rights, do not train teachers to identify cyberbullying or online exploitation, and fail to engage parents in digital safety training.

5. Weak Content Moderation in Regional Languages: AI moderation tools used by platforms often fail to catch abuse, threats, or grooming when content is in non-English Indian languages, leading to underreported harm in rural and regional communities.

Emerging Challenges in the Digital Landscape –

1. Rise of Deepfakes and Synthetic Media: AI-generated deepfakes threaten children's dignity and privacy. These manipulated images or videos can be used for online bullying, revenge pornography, and sextortion, especially targeting teenage girls. Current legal tools are ill-equipped to criminalise or remove deepfake content swiftly, especially when hosted on foreign servers.

2. Digital Addiction and Mental Health: Children, especially in urban and semi-urban areas, face screen addiction, leading to sleep disorders and social withdrawal, dopamine manipulation via short videos, endless scrolls, and likes and gaming disorders, classified by WHO as a behavioural condition.

3. Dark Web and Online Trafficking: Children are increasingly vulnerable to identity theft through leaked Aadhaar and academic data, recruitment for illicit purposes via online platforms, and exposure to pornographic networks or online drug marketplaces.

4. Commercial Exploitation via Influencer Culture: Currently, child influencers may make money without labour protection, income monitoring, or psychological protection against exhaustion or overexposure. In India, there is no clear provision under the labour law or advertising codes to address digital child labour.

5. Algorithmic Bias and Data Discrimination: Children from marginalised communities may be exposed to low-quality, stereotypical content, excluded from advanced educational algorithms and face long-term digital inequality due to biased AI systems. Without proper audits and transparency, these algorithms risk deepening social divides rather than bridging them.

RECOMMENDATIONS AND WAY FORWARD

1. Enact a Child Online Safety and Empowerment Act: A standalone law for child digital rights should define harmful content and abusive behaviours, make age-appropriate design mandatory, set up a regulatory authority for oversight and include fast-track grievance mechanisms.

2. Strengthen Institutional Architecture: Establish a Children's Digital Rights Commission with investigative powers, cross-platform compliance monitoring, and emergency content takedown abilities. This body can liaise with NCERT, NCPCR, MeitY, and international watchdogs.

3. Mandate Age-Gating and Privacy-by-Design: Laws should enforce default privacy settings for users under-18, ban behavioural advertising to minors and require apps to use verified, ethical age-gating technologies.

4. Make Digital Citizenship a Core Curriculum: The NCERT and state boards should incorporate awareness of digital rights and responsibilities, skills to identify cyber threats, ethical use of AI, data, and online safety training modules for teachers and parents.

5. Invest in Child-Sensitive AI and Local Language Tools: India should fund open-source AI for content moderation in major Indian languages, early detection of child grooming or bullying and adaptive learning platforms that avoid bias.

6. Recognise and Regulate Child Influencers: Update labour and advertising laws to limit screen time and production hours, mandate guardian oversight and savings accounts for child earnings, and ban exploitative product placements targeting child audiences.

7. Create Digital Rehabilitation and Counselling Services: Include cyber trauma and digital addiction in school counselling programs, district Child Protection Units (CPUs) and tele-mental health initiatives under the Ayushman Bharat scheme.

CONCLUSION

The digital era has revolutionised childhood. Modern children are raised in the era of smartphones, artificial intelligence, virtual school, and social media, which provide new possibilities and potential threats. India has made progress in recognising and protecting children's rights via its constitutional and statutory framework, but there are significant gaps between legal visions and digital reality.[42] This study highlights that children are more vulnerable to internet abuse, cyberbullying, exploitation, algorithmic manipulation, and data surveillance.

The advancement of technology is faster than the laws. The lack of child-specific digital rights legislation and central regulatory power is a major concern. Additionally, low awareness, limited age-appropriate design in digital platforms, and an insufficient digital literacy education system enhance the digital gap and safety issues. By providing children with safe opportunities for learning, creativity, and socialisation, they can navigate the digital world responsibly. Ensuring safe, fair, and informed participation is a more effective solution than restricting internet access. A rights-based, child-centric approach that combines empowerment, security, independence, and creativity with responsibility is urgently needed.

[42] Anum Naz and Kainat Ahmed, 'Digital Safety for Kids: A Strategic Guide for Parents in the Digital Age' (2024) SSRN <https://dx.doi.org/10.2139/ssrn.5067317> accessed 13 May 2025