INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 8 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 8 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-7-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

GROWING UP ONLINE: SAFEGUARDING CHILDREN'S RIGHT IN DIGITAL PLAYGROUND

AUTHOR - SUMIT PANDEY, STUDENT AT UNIVERSITY OF DELHI

BEST CITATION - SUMIT PANDEY, GROWING UP ONLINE: SAFEGUARDING CHILDREN'S RIGHT IN DIGITAL PLAYGROUND, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (8) OF 2025, PG. 750-763, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

In the digital era , the use of internet for study , recreation and social interaction is growing among children. This connectedness has many advantages but it also create problems that disproportionately harm children owing their fragility and ignorance. Cyberbullying, Online Gaming, Data abuse , AI generated deepfakes and hazardous material pose are several examples which are harmful to children and it requires urgent legal , technical and social remedies.

This article critically analyse the global and Indian child's rights and safeguard in the digital world and also examines how UNCRC , Information Technology Act 2000, Protection of Children form Sexual Offence 2012 and Digital Personal Data Protection Act 2023 deals with these challenges. This article also examine the landmark case laws , Policy gaps and current issue like AI and misinformation. Alongwith, from child- centric view, this article discuss the need for balanced strategy & regulations which protects children's right to access information and express themselves online while preserving their safety , privacy and dignity. A systematic change includes legal protection, ethical digital practices , public awareness and education.

Keywords: Children, Privacy, child's safety, Artificial intelligence,

Introduction

21st century is witness of unprecedented digital revolution which transform the people's way of life, learning and communication. The children, whose early years are being more influenced by technology, are among those who mostly impacted by this change.By online classroom, online games, video sharing platform and learning aids driven by Artificial intelligence, nowadays, children are engrossed in virtual world which is both powerful and dangerous.

By the advancement of technologies children have so much possibilities at their fingertips. Instantaneous information, worldwide peer connection and opportunity to develop employable skill are all within their reach . Cyberbullying, identity theft, exploitation, misinformation and psychological discomfort due to excessive screen time or algorithm driven content are the some examples which may expose the child by using the same tools which empower them. The line between benefits and risk is very thin in case of child who can't completely understand the consequence of his online activity.[789]

The issue of children's internet safety has become more prominent on global scale. Child welfare organizations and UNICEF have found that internet abuse and exploitation are on rise[790]. The Covid-19 pandemic further accelerated the children's screen dependency and vulnerability, which shifted their social and

[789] Sharma, A. (2010) , 'Globalization and its impact on cyber crime: A case study of Indian police administration', Indian Journal of Public Administration,56(2) <http://doi.org/10.1177/0019556120100203> accessed 11-05-2025

[790] Etter , B. (2001), 'The forensic challenges of e-crime', Current Commentary No. 3 Australasian Center for Policing Research , Adelaide

educational environment into online domain.This has made the protection of children in cyber space an important matter of public policy , law and child rights.

In India, the internet users are growing rapidly which generates unique problems. Everyday, millions of youngsters use the internet; thus, the country's legal framework has evolved to accommodate these new realities. The right to privacy and digital well- being is implicitly include in the right to life & dignity guaranteed under Article-21 of Constitution[791]. However, there are large protection gaps in current laws which struggle to match with speed of technological change.

This research article aims to fill these gaps by examining the rights & protection that children have in the in the digital era. It looks at current laws , evaluate new cyber danger and talks about how the courts and government are reacting to them . By focusing on child-first approach, this article underscore how critical it is to build more robust and future ready system which empower and protect them in equal measure.

Ultimately, the protection of children in digital era, is more of social needs than technological or legal one. When country takes measures to ensure the safety of its younger users ,it shows that it supports democratic values, human dignity and inclusive development. Innovation must co-exists with integrity, freedom co-exists with responsibility and access must co-exists with accountability if we are to progress.[792]

Legal Foundation of Child's Rights in digital sphere

- **International framework**
  - **United Nations Convention on Right of Child (UNCRC)**[793]

The cornerstone of child's rights at international level is UNCRC , adopted in 1989. While it predates the digital revolution, its principles are still highly relevant in digital age . Article 13, 16 and 17 of UNCRC directly pertain to child's freedom of expression, protection from arbitrary interference with privacy and access to appropriate information though mass media.

General Comment no. 25 of UNCRC[794] was presented in 2021 which deals with issue of child's rights in digital environment. This document emphasizes the need of safeguarding child's rights online just as they are offline. It demands the creation of laws , policies and environment which provides fair access to digital resources , protect users from online danger and encourage digital literacy and safety.

- **Sustainable Development Goals**[795]

The Sustainable Development Goals (SDGs) was adopted by United Nations in 2015 aims to ensure a better and more sustainable future for all by 2030 . There are several SDGs goals on protecting child in digital sphere.

1. **SDG 3, Good Health and Well-being:** Promote mental health by preventing online bullying, screen addiction and social media pressure.
2. **SDG 4, Quality Education:** Ensure all children have equal access to quality online learning platform and digital tools
3. **SDG 16, Peace, Justice and Strong Institution:** Protect children from abuse, exploitation, trafficking and Violence against them in real and digital sphere.
4. **SDG 17, Partnership for Goals:** Government, Tech-companies , Schools and families must work together to

[791] The Constitution of India
[792] Choucri, N & Goldsmith , D. (2012), 'Lost in cyberspace: Harnessing the internet' , international relation & global security. Bulletin of Atomic Scientists, 68(2) <http://doi.org/10.1177/0096340212438696>accessed 11-05-2025
[793] United Convention on Rights of Child , 1989 <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> accessed 7-05-2025
[794] General Comment No. 25 (2021) on Children's Rights in Relation to Digital Environment <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation> accessed 7-05-2025
[795] The 2030 Agenda for Sustainable development

make the internet safer and fair for children.

- **ECOSOC Resolution 2011/33**[796]

"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 children19" is resolution issued by the United Nation Economic and Social Council. The resolution drafted a study that how these information technologies and other electronic technologies are affected crimes against children.

- **The Rio de Janeiro Duration**[797]

The "Third World Congress" against the children's exploitation was held in Rio De Jeneiro in Brazil in year 2008. The aim of the declaration was to take such a effective step to combat the sexual exploitation against children. The Declaration focused on the reasons and causes of the sexual exploitation of children and discussed the strong and broader strategies like "Millennium development Goals 21" to prevent and combat this crime by eradication "extreme poverty and hunger".

- **Indian Constitutional & Legal Provision**
  - **The Constitution of India**
    - **Art 21:** Guarantees the right to life & personal liberty, which courts have interpreted to include right to privacy, education and digital safety.
    - **Art 39(e) & (f) :** The direction under Directive Principles of State Policy is for the State to ensure that children are not abused & that their childhood is protected.
    - **Art 45:** State ensures early childhood care and education for all children until they complete the age of six years.
  - **Information Technology Act**[798]

    The IT Act is India's primary cyber law . Some of the Section are child specific -
    - **Sec-66E:** Punishes violation of privacy through capturing, publishing or transmitting private imges without consent.
    - **Sec-67B:** Specially criminalizes the publishing, browsing or downloading of child sexual abuse material.
    - **Sec-69A:** Grants government power to block content harmful to public including children.
  - **Protection of Children from Sexual Offences**[799]

    This Act is comprehensively addresses the sexual offences against child including those facilitated by digital means.
    - **Sec-11 & 12:** Address sexual harassment which includes sending lewd messages or engaging in online sexual communication.
    - **Sec-15:** includes provision to penalize the storage or possession and distribution of child sexual abuse material.

[796] Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children (E/2011/30)
[797] 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 (November, 2008).
[798] The Information Technology Act , 2000
[799] Protection of Children from Sexual Offences 2012

- **Juvenile Justice Act**[800]

  While primarily a welfare legislation, it mandates the State to protect children from abuse, neglect and exploitation in all settings including online environments.

- **Digital Personal Data Protection Act**[801]

  This recent legislation makes a crucial development in digital rights landscape. It introduces the concept of 'verifiable parental consent' for processing data of minors .

  Key highlights:

  - No tracking, targeted advertisement or data monetization is allowed for user under 18 years 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
    - Responsible social media use

  - **OTT and Social Media self regulation** [802]

    Platform like YouTube , Meta, Prime and Netflix have introduced restricted modes , content rating system and child specific applications. However, many of these remain optional and depends 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 just as damaging[803]. By increasingly using of the internet for education, communication, and entertainment, children also become vulnerable to dangers which challenges their safety, privacy, emotional well-being, and even their development. Followings are emerging threats in detail.[804]

- **Online Sexual Exploitation and Abuse**

  One of the gravest threats faced online by children is sexual exploitation and abuse. Sometimes over long periods, criminals groom children by gaining their confidence via social media, messaging applications, and online gaming platforms.

  Forms of Exploitation:

  1. Child Sexual Abuse Material (CSAM): Explicit images or videos of child being shared or sold

[800] Juvenile Justice (Care and Protection of Children) Act, 2015
[801] Digital Personal Data Protection Act, 2023
[802] Advisory on adherence of Indian Laws and the Code of Ethics prescribed under the Information Technology (Intermediary Guidelines and Digital Media, Ethics Code) Rules, 2021
[803] Bernik , I.(2014), 'Cybercrime & Cyberwarfare' <https://doi.org/10.1002/9781118898604.ch1> accessed 7-05-2025
[804] Mokha , Anupreet. (2017), 'A study on Awareness of cybercrime and security', Research J. Humanities and Social Sciences. 8(4) doi: 10.5958/2321-5828.2017.00067.5

online. According to Interpol and reports by NGOs, India has seen a steep rise in CSAM circulation.[805]

2. Live-streamed abuse: It will become more difficult to identify and prosecute offenders when they make live-stream abuse.
3. Grooming: Offenders often create fake profiles and lure children into inappropriate relationships, sometimes leading to blackmail (sextortion).[806]

- **Cyberbullying and Online Harassment**

Cyberbullying has become increasingly common among children and teens. It includes:

1. Sending threatening or abusive messages
2. Posting embarrassing photos or videos
3. Spreading rumors on social media

Extreme occurrence of cyberbullying may result in suicidal thoughts, desperation, social withdrawal, and anxiety. Some platforms do not have real-time monitoring and do not have reporting systems that are suitable for children, which makes it more difficult for victims to seek aid[807].

- **Privacy Invasion and Data Exploitation**

Children often use applications and platforms that collect personal data, sometimes without their or their parents' knowledge.

Key concerns:

1. Surveillance-based advertising: Online behavior of children is tracked and used to create marketing profiles, which violates their privacy.
2. Lack of informed consent: Children may not understand what they are agreeing to when apps request permissions.
3. Data breaches: When educational platforms or gaming apps get hacked, sensitive data related to child can be leaked or sold on the dark web.

- **Exposure to Inappropriate Content**

Children may stumble upon or be exposed to:

1. Violent or graphic media
2. Pornographic content
3. Self-harm or suicide-related discussions (e.g., Blue Whale Challenge)
4. Misinformation and conspiracy theories

Algorithms on platforms like YouTube or TikTok often auto-suggest such content, creating echo chambers that worsen mental health outcomes. Parental controls exist but are often complex or bypassed.

[805] Ali, Sana & Haykal, Hiba . (2021). 'Child Sexual Abuse and the Internet—A Systematic Review'. Human Arenas DOI:10.1007/s42087-021-00228-9

[806] Schoeps, Konstanze & Montserrat, Peris,. (2020).'Risk factor for being a victim of online grooming in adolescents'. Psicothema. 32. DOI: 10.7334/psicothema2019.179

[807] Singh, Swarndeep & S& Sagar, Rajesh. (2022). 'Quality of online news media reports of child sexual abuse in India'. Industrial Psychiatry Journal. 31 DOI:10.4103/ipj.ipj_238_21

- **Radicalization and Extremist Propaganda**

  Some children are targeted by extremist groups online to influence their thinking and behavior. These groups use:

  1. Encrypted platforms and chat rooms
  2. Memes and gamified propaganda
  3. 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.[808]

- **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:

  1. Gaming addiction, leading to poor academic performance and disturbed sleep
  2. In-game purchases causing financial exploitation
  3. Exposure to gambling mechanics (loot boxes, betting apps) under the guise of 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:

  1. Sextortion
  2. Bullying
  3. False accusations
  4. Manipulated consent videos

- **Misinformation and Algorithmic Bias**

  Children often rely on social media or unverified sources for information. Misinformation campaigns can:

  1. Distort their worldview
  2. Promote hatred or discrimination
  3. Encourage unhealthy behavior (fake health cures, diet trends, etc.)

  Even algorithms have the potential to show biased material, which may amplify prejudices and suppress diversity. As an example, biased image suggestions and beauty filters have the potential to damage social identity and self-esteem.[809]

- **Online Radical Gender or Racial Narratives**

  There are a lot of extreme gender or racial narratives that teenagers see online.. These include:

  1. Incels (involuntary celibates) communities which promote misogyny.
  2. Hates groups who promote racist ideologies.
  3. Toxics beauty standards which marginalize certain races or ethnicities.

  Without the ability to think critically and the encouragement of adults , children

[808] Bada Maria, Nurse R.C.(2019) ,'The social & psychological impact of cyber attack', Benson V., & Mcalaney J. (Eds.), Emerging cyber threats and cognitive vulnerabilities , 73–92 <https://doi.org/10.1016/B978-0-12-816203-3.00004-6> accessed 12-05-2025

[809] Shin, Donghee. (2024). 'Artificial Misinformation: Exploring Human-Algorithm Interaction Online'. DOI: 10.1007/978-3-031-52569-8.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

can internalize these messages and mirror harmful behavior.[810]

- **Psychological and Developmental Impact**

  The cumulative effect of these threats manifest in

  1. Attention deficiency and low cognitive ability.
  2. Poor social attraction due to over dependence on virtual attraction.
  3. Anxiety , depression and identity confusion.
  4. Sleep disorder & behavioral change.

  Over use of screens also lead to physical issues like vision problems , obesity and posture related complications.[811]

- **Parental and Institutional Challenges**

  Many parents don't know what their kids are up to on the internet. Key obstacles include:

  1. No digital or computer knowledge among guardians
  2. Digital safety education in schools are limited
  3. Over-reliance on paid parental control softwares and tools
  4. Trust deficit between children and caretakers

  Unfortunately, many schools don't have any cyber counselors or secure reporting channels, which makes it even more difficult for children to come and share their experience about online harassment.

Institutional and Civil Society Initiatives

Protecting children in India from harm while they are online is a shared duty across several sectors of society. In an effort to create a more secure online space, many public agencies, nonprofits, and even for-profit businesses are working together.

- **Government Initiatives**

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

  1. **National Commission for Protection of Child Rights (NCPCR):** In developing cyber safety standards for children, the role of NCPCR are very crucial . In a joint advisory with MeitY, it lays out steps that parents, schools, and social media companies may do to combat child abuse on these platforms.
  2. **Cybercrime Prevention against Women and Children (CCPWC) Scheme:** The Ministry of Home Affairs launched this plan to assist states and UTs in enhancing their cybercrime units. Additionally, it provides funding for programs that aim to raise awareness and strengthen capacities.
  3. **Digital India Programme:** Though it does not child-specific, it does have digital literacy programs like "PMGDISHA (Pradhan Mantri Gramin Digital Saksharta Abhiyan)" that may be used to educate families and children on fundamental digital hygiene.[812]
  4. **Cyber Crime Reporting Portal (https://cybercrime.gov.in):** This

[810] Gopal, Pragathi. (2012). 'Literary Radicalism in India: Gender, Nation and the Transition to Independence. Literary Radicalism in India: Gender, Nation and the Transition to Independence'. DOI: 10.4324/9780203391174.

[811] Bada Maria, Nurse R.C.(2019) 'The social & psychological impact of cyber attack', Benson V., & Mcalaney J. (Eds.), Emerging cyber threats and cognitive vulnerabilities , 73–92 <https://doi.org/10.1016/B978-0-12-816203-3.00004-6 > accessed 12-05-2025

[812] Tiwari, Amit & Varadarajan, Udaya , (2017), 'Digital India initiatives : An educational panorama' .

portal gives a platform to anyone (including children and parents), to report offence like cyberbullying, grooming, or exploitation .. etc. The portal has a separate tab for reporting child sexual abuse material (CSAM).[813]

- **NGO and Civil Society Efforts**

There is a critical shortage of resources to address children's digital safety, but several non-governmental organizations (NGOs) in India are actively trying to fill this void via education and protection.

1. **CyberPeace Foundation:**.For the benefit of children in underserved and rural regions, this non-governmental organization (NGO) collaborates with the Indian government and UNICEF to provide workshops on digital literacy. Its "CyberPeace Clubs" program promotes in-school collaborative learning on topics such as cyberbullying, online grooming, and disinformation.
2. **Save the Children India:** They run several projects focused on online safety awareness, especially targeting adolescent girls vulnerable to online exploitation and cyberstalking.
3. **Bachpan Bachao Andolan:** While this group has long worked to end the exploitation and trafficking of children, they have recently shifted their attention to the ways in which the internet and other forms of digital communication affect children's rights and protection.
4. **Childline India Foundation (1098):** Primarily, this is a women protection helpline but it also receives cases related to online abuse and exploitation of child . It provides immediate intervention and referrals.

- **Public-Private Partnerships and EdTech Platforms**

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

1. **Meta (Facebook, Instagram):** Meta has launched a 'Parent's Guide' for Instagram in India in partnership with organizations like Aarambh India Initiative. It educates parents and teens about safe usage.
2. **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.
3. **EdTech Platforms:** Companies like BYJU'S, Vedantu, and others are increasingly embedding content moderation and child-safety tools, although a standardized child-safety policy across platforms is still lacking.

- **School-Based Initiatives**

Recognizing schools as key stakeholders, the government has:

1. Introduced cyber safety modules under the Digital India initiative.
2. Launched programs like Cyber Surakshit Bharat and Information Security Education & Awareness (ISEA) for students and teachers.

[813] Chhabra, Dr. (2020). 'Rights of children in cyber world Indian perspective'.

3. Promoted CBSE advisories on digital etiquette and the safe use of social media.

- **Role of Intermediaries and Tech Platforms**

  Under the IT Rules (2021), platforms are required to:

  1. Remove objectionable content within 24 hours of complaint.
  2. Deploy AI-based content moderation.
  3. Appoint grievance officers for faster redressal.

- **Judicial Interventions**

  The Indian judiciary has played an active role in expanding digital protections: Through various judgements , Courts also protects the children's rights in digital sphere & reshaping the digital environment.

  Case- Avnish Bajaj v. State (2005 Delhi High Court) [814]

It is first major case on intermediary liability for content related to child. In this case , the court highlighted intermediary's liability in distribution of obscene material involving minors.

Case- Shreya Singhal v. Union of India (2015 SC)[815]

This landmark ruling which declares sec-66A of Information Technology Act 2000 , Unconstitutional and laid foundation for protection of minors from vague digital criminal law.

Case- In Re : Prajwala Letter Case (2017)[816]

This case is related to circulation of rape & child pornography videos online. The Hon'ble Court issue direction to government and tech companies to develop mechanism for removing child sexual abuse material.

Case- In Re: Children in Street Situation (2022)

In this case Hon'ble Court recognized the need for safe digital access, identity-linked entitlements and online education safeguards

Case - Facebook India Online Service Pvt. Ltd. v. Union of India (pending)

This case underscore the balance between privacy and safety, especially in protecting children from online sexual exploitation, cyberbullying and grooming. It highlighted the accountability of platform in removing & preventing spread of CSAM

Case- Just Rights for Children Alliance v. S. Harish (2024)[817]

This case highlighted the urgent need to protect children from online abuse and exploitation. The court emphasized creating robust digital safeguards, holding platform accountable and ensuring children's rights to safety, dignity and privacy in digital environment.

International Perspectives and Best Practices

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

- **European Union's General Data Protection Regulation (GDPR)**[818]

  The GDPR has strict rules for 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. Its "age-appropriate design code" in the UK mandates privacy-by-default settings for minors.

[814] 2005(79)DRJ576
[815] AIR 2015 SC 1523
[816] 2018 LawSuit(SC) 285
[817] 2024 INSC 716
[818] General Data Protection Regulation (Regulation (EU) 2016/679) <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://gdpr-info.eu/&ved=2ahUKEwiYno3io6CNAxVnqVYBHdLWM6cQFnoECHAQAQ&usg=AOvVaw1akHzzz224Oq1yU0pd6qSw> accessed 12-05-2025

While the Digital Personal Data Protection Act, 2023 in India does provide similar safeguards, it does not yet mandate impact assessments for digital services targeted towards children or establish explicit methods for verifying their age.

- **United States: Children's Online Privacy Protection Act (COPPA)**[819]

  In order 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 criticized for failing to adapt to new types of data collecting 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**[820]

  This law empowers the eSafety Commissioner to:

  - Make order to remove harmful content, including cyberbullying and image-based abuse.
  - Offer to make a reporting tool for youth experiencing online harm.
  - Regulate online platforms with a safety code of conduct.

  It gives One-stop grievance redressal which combined with strong enforcement and platform accountability.

  Lesson for India: The idea of a separate agency responsible for children's internet safety, might help Indian organizations consolidate their fragmented governance structures.

- **South Korea: Digital Well-being and Screen Time Regulation**[821]

  South Korea adopts a technocultural approach:

  - By law, smartphone sold to minors must have parental controls installed in order to avoid smartphone addiction.
  - Government funded digital detox camps and cyber wellness education.

  It makes balance between protection with mental health promotion and digital literacy.

  Application in India: Similar behavioral support programs in schools could reduced the overuse and online gaming addiction.

- **Global Guidelines: UNICEF and ITU Frameworks**[822]

  UNICEF's "Children's Rights in the Digital Age Report" and the International Telecommunication Union (ITU) guidelines serve as global references:

  - Highlight the importance of children's involvement in the process of developing regulations about digital infrastructure.
  - Strongly encourage governments to prioritize equal access and digital inclusion.
  - Raise awareness about AI policies that protect children in order to prevent algorithmic bias.

[819] Children's Online Privacy Protection Act of 1998 <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim> accessed 13-05-2025

[820] Online Safety Amendment (Social Media Minimum Age) Act 2024

[821] Woo, Kyung & Bong, (2021). 'Mental Health, Smartphone Use Type, and Screen Time Among Adolescents in South Korea. Psychology Research and Behavior Management'. DOI:1419-1428. 10.2147/PRBM.S324235.

[822] Guidelines for industry on Child Online Protection 2020 <https://www.unicef.org/media/90796/file/ITU-COP-guidelines%20for%20industry-2020.pdf> accessed 13-05-2025

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

India: India has been an active partner in these forums, but could 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:

- **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.
- **Child Helpline International:** Supports cross-border emergency assistance for digital child abuse cases.

Takeaway for India: There is potential for stronger public-private partnerships to create localized tools and platforms that meet India's linguistic and cultural diversity

- **Technological Interventions in Other Countries**

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 behavior on children's gaming platforms.
- New Zealand collaborates with tech firms to use image hashing to fight child sexual abuse material (CSAM).

India's Opportunity: Invest in ethical AI systems for content moderation, real-time threat detection, and localized 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.In this part, we will look at the policy gaps, potential problems, and proposed reform strategy 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 provision, none is specifically deals 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
- Limited child-specific redressal mechanisms

2. Inadequate Age-Verification Standards

India lacks mandatory, standardized age-verification tools across platforms. As a result:

- Children easily access age-inappropriate content (e.g., violent games, adult media)
- Apps collect sensitive data from minors without valid consent

3. No Regulatory Body for Child Digital Welfare

Unlike Australia's eSafety Commissioner, India has no central authority focused solely on 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 digital rights education
- Do not train teachers to identify cyberbullying or online exploitation
- Do not 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
- Sextortion, especially targeting teenage girls

Current legal tools are ill-equipped to criminalize 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
- Gaming disorders, classified by WHO as a behavioral condition

3. Dark Web and Online Trafficking
Children are increasingly vulnerable to:

- Using leaked Aadhaar and academic data to commit identity theft
- Recruiting for illicit purposes using online platforms
- Being exposed to pornographic networks or online drug marketplaces

4. Commercial Exploitation via Influencer Culture
Currently, child influencers may make money without:

- Labour protection
- Income monitoring
- Psychological protections against exhaustion or overexposure

In India , there is no clear provision under labor law or advertising codes to address digital child labor.

5. Algorithmic Bias and Data Discrimination
Children from marginalized communities may:

- Receive low-quality, stereotypical content
- Be excluded from advanced educational algorithms
- Face long-term digital inequality due to biased AI systems

Without audits and transparency, algorithms may deepen social divides rather than bridge them.

- **The Road Ahead: Strategic Recommendations**

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1. Enact a Child Online Safety and Empowerment Act

A standalone law for child digital rights should:

- Define harmful content and abusive behaviors
- Make age-appropriate design mandatory
- Set up a regulatory authority for oversight
- Include fast-track grievance mechanisms

2. Strengthen Institutional Architecture

Establish a Children's Digital Rights Commission with:

- Investigative powers
- Cross-platform compliance monitoring
- 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 under-18 users
- Ban behavioral advertising to minors
- 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 spaces
- 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
- Adaptive learning platforms that avoid bias

6. Recognize and Regulate Child Influencers

Update labor and advertising laws to:

- Limit screen time and production hours
- Mandate guardian oversight and savings accounts for child earnings
- Ban exploitative product placements targeting child audiences

7. Create Digital Rehabilitation and Counseling Services

Include cyber trauma and digital addiction in:

- School counseling programs
- District Child Protection Units (DCPUs)
- Tele-mental health initiatives under the Ayushman Bharat scheme

Conclusion

The digital era has revolutionized childhood. Modern children are raised in a era of smartphones , Artificial Intelligence, virtual schools, and social media, which provide new possibilities and also potential threats. India has made progress in recognizing and defending children's rights via its constitutional and statutory framework , but there is

substantial gap between legal visions and digital reality[823].

This study shows that children are more vulnerable to internet abuse, cyberbullying, exploitation, algorithmic manipulation, and data surveillance. The advancement of technology is faster than laws. Lack of a child-specific digital rights legislation and central regulatory power are major concern. Additionally, low awareness, limited age-appropriate design in digital platforms, and insufficient digital literacy education system enhance the digital gap and safety issues.

By providing many chances for learning, creativity, and socialization, children can safely navigate the digital world. Safe, fair, and informed involvement is the solution instead of limiting children's internet access. A rights-based, child-centric strategy that combines empowerment, security, independence, and creativity with responsibility is needed now.

[823] Naz, Anum and Ahmed, Kainat. (2024) , 'Digital Safety for Kids: A Strategic Guide for Parents in the Digital Age', <https://dx.doi.org/10.2139/ssrn.5067317> accessed 13-05-2025