INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CHILDREN'S DIGITAL PRIVACY AND CYBER SAFETY IN INDIA: LEGAL CHALLENGES AND EMERGING CONCERNS.

AUTHORED BY - RESHMA R
LLM
Sree Narayana Law College, Ernakulam, Kerala.

Abstract

The increasing use of digital platforms by children in India has created serious concerns regarding cyber safety and online privacy. Children today are exposed to various online risks, including cyber bullying, online grooming, identity theft, data misuse, sextortion, and exposure to harmful content through social media, gaming applications, and educational platforms. This paper examines legal and constitutional framework relating to protection of children in digital spaces in India. It analyses important legislations such as the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023. The paper also discusses emerging technological threats including artificial intelligence, deepfake technology, and online data exploitation. Further, it highlights socio-legal challenges such as weak enforcement, lack of digital awareness, and increasing cyber-crimes against children. The study concludes with recommendations for strengthening child online protection mechanisms and digital privacy safeguards in India.

Keywords

Cyber Safety, Children's Privacy, Online Exploitation, Cyber Laws, Digital Rights, Child Protection, Data Privacy, POCSO.

Introduction

Internet is an excellent source of learning, shopping, playing games or staying connected with friends; but there is always an implied risk of falling victim to various online threats every time you browse the web. Children & teens are the most susceptible to this as there are predators, identity thieves, hackers, and others who can make you end up losing your personal information & privacy. The internet has seen significant growth in India, with children aged 5-11 making

ISSN: 2582-6433

up 14% of active users, as reported by the Internet and Mobile Association of India.[1]

The rapid growth of digital technology has significantly transformed the social and educational environment of children in India. Increased internet accessibility, affordable smartphones, online learning platforms, social media applications, and digital gaming environments have enabled children to engage extensively with cyberspace. While digital technology has created opportunities for education, communication, and creativity, it has also exposed children to serious online risks such as cyberbullying, cyber grooming, sextortion, identity theft, exposure to harmful content, and misuse of personal data. The growing dependency on digital platforms has therefore raised important concerns regarding children's cyber safety and online privacy.

Children are particularly vulnerable in digital spaces because of their limited understanding of online risks, emotional susceptibility, and lack of digital literacy. Social media companies, gaming applications, and educational technology platforms often collect and process large amounts of children's personal information, including photographs, browsing behavior, location data, and biometric details.[2] Such large-scale data collection increases the risk of privacy violations, online manipulation, and cyber exploitation. Emerging technologies such as artificial intelligence, deepfake technology, and algorithmic profiling have further intensified concerns regarding the protection of children's digital rights.

The Indian constitutional framework recognizes the protection of dignity, liberty, and privacy as integral components of fundamental rights guaranteed under Article 21 of the Constitution of India. The landmark judgment in Justice K.S. Puttaswamy v. Union of India recognized privacy as a fundamental right and emphasized the importance of informational privacy in the digital age.[3] In addition, several legislations including the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, the Juvenile Justice (Care and Protection of Children) Act, 2015, and the Digital Personal Data Protection Act, 2023 provide legal safeguards against online exploitation and privacy violations affecting children.[4]

[1] Economic Times, "India has over 500 mn active internet users, 14% of 5-11 yrs: IAMAI", available at: https://m.economictimes.com/tech/internet/india-has-over-500-mn-active-internet-users-14-of-5-11-yrs-iamai/articleshow/75556305.cms (last visited on May 12, 2026).
[2] Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing Co., New Delhi, 5th edn., 2016) at 87.
[3] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[4] Information Technology Act, 2000; Protection of Children from Sexual Offences Act, 2012; Digital Personal Data Protection Act, 2023

ISSN: 2582-6433

Despite the existence of these legal protections, effective implementation remains a major challenge. Rapid technological advancement, weak enforcement mechanisms, underreporting of cyber offences, lack of awareness among parents and children, jurisdictional difficulties, and cross-border cybercrimes continue to hinder effective child protection in cyberspace.[5] Consequently, there is an urgent need for stronger legal regulation, digital literacy, institutional accountability, and child-centric cyber safety policies in India.

CYBER SAFETY

Cyber safety revolves around protecting individuals and users in the digital space, emphasizing the responsible and ethical use of technology. It encompasses measures to ensure a positive online experience, free from harm, harassment, or exploitation. Cyber safety is particularly pertinent in the context of individuals, children, and vulnerable groups navigating the internet. It involves strategies to prevent cyber bullying, secure online transactions, and promote digital well-being.

One of the key components of cyber safety is education. Promoting digital literacy empowers individuals to navigate the online world safely, recognizing potential risks and adopting responsible online behaviour. Cyber safety extends beyond the conventional cyber security measures, emphasizing the human factor in mitigating digital threats.

Addressing the human element in cyber safety involves creating awareness about the consequences of online actions, understanding privacy settings, and promoting a respectful online environment. Cyber safety initiatives often extend to families, schools, and communities, emphasizing the importance of being a responsible digital citizenship and ethical online conduct.[6]

Child Rights in Digital Space

The rapid growth of digital technology has considerably influenced the lives of children in India, as they increasingly use online platforms for education, communication, gaming, and entertainment. Although digital technology provides valuable opportunities for learning and

[5] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn. 2022) at 245.
[6] US Cybersecurity Magazine, "Unraveling the Distinctions Between Cyber Safety and Cyber Security", available at: https://www.uscybersecurity.net/csmag/unraveling-the-distinctions-between-cyber-safety-and-cyber-security/ (last visited on May 12, 2026).

ISSN: 2582-6433

social interaction, it also exposes children to various risks such as cyberbullying, online exploitation, privacy violations, and harmful digital content. Consequently, the protection of child rights in digital spaces has become an important socio-legal concern. Child rights in the digital environment include the right to privacy, dignity, education, safe access to information, and protection from exploitation. Owing to limited digital awareness and emotional vulnerability, children are more susceptible to online manipulation and cyber threats. Furthermore, social media platforms, gaming applications, and other digital services often collect and process children's personal data, thereby raising concerns regarding misuse of information, surveillance, and online exploitation.[7]

Types of Cyber Risks

Children face significant cyber risks including cyberbullying, online grooming, exposure to inappropriate content and privacy breaches, with over 60% of children (8-12) exposed to online threats. . These risks often appear via social media, gaming and messaging platforms. The main types of cyber risks are;

1. **Cyber Grooming**

   Cyber grooming refers to the process in which an individual, usually an adult, establishes an online relationship with a child or young person for the purpose of sexual exploitation, abuse, or trafficking. Offenders often create fake identities and approach children through social media, gaming platforms, or child-friendly websites by engaging in casual conversations about hobbies, school, or family to gain their trust and emotional confidence. They may also offer gifts, emotional support, guidance, or financial benefits to manipulate children. Once trust is developed, groomers frequently persuade children to share intimate photographs, videos, or engage in sexually explicit conversations, which may later be used for coercion or blackmail. In some cases, offenders attempt to arrange physical meetings for abusive purposes, while children may unknowingly become vulnerable through online platforms offering rewards or incentives in exchange for personal information or intimate content.[8]

[7] UNICEF, *Children's Rights in the Digital World* 25 (2017); Shubhankar Dam, *Cyber Law and Child Protection in India* 112 (Eastern Book Company, Lucknow, 2018).
[8] Child Safe Net Foundation, "Cyber Grooming", available at: https://www.childsafenet.org/cyber-grooming (last visited on May 15, 2026).

ISSN: 2582-6433

2. **Cyberbullying**

Cyberbullying refers to bullying or harassment carried out through digital technologies such as social media platforms, messaging applications, gaming platforms, and mobile devices. It involves repeated behaviour intended to intimidate, humiliate, threaten, or emotionally harm another person. Cyberbullying may include spreading false information, sharing embarrassing photographs or videos online, sending abusive or threatening messages, impersonating individuals through fake accounts, or posting harmful content in another person's name. With the advancement of technology, cyberbullying has also expanded to include the use of generative artificial intelligence tools for harassment, manipulation, and online abuse, including the creation of harmful or inappropriate digital content targeting individuals.[9]

3. **Sextortion**

Sextortion is a form of blackmail in which the attacker threatens to send sexual images or videos of you to others if you do not pay them or give them additional sexual content. This sextortion definition applies to any gender, and although attacks can be directed at anyone of any age, attackers tend to target younger individuals.

A sextortion predator uses the fear of embarrassment against their victims. Knowing their targets do not want any humiliating content on the internet, they use threats to motivate young people into giving them money. Attackers may also threaten to send the images to the victim's parents, school officials, or even their employers unless the target either pays them or sends more content.[10]

4. **Identity Theft**

Identity theft occurs when a person unlawfully obtains and uses another individual's personal information for personal gain without consent. It can take various forms and may negatively affect the victim's reputation, financial security, credit status, or future opportunities. Even individuals without significant financial assets can become targets,

[9] UNICEF, "How to Stop Cyberbullying", available at: https://www.unicef.org/stories/how-to-stop-cyberbullying (last visited on May 15, 2026).
[10] Fortinet, "What is Sextortion?" available at: https://www.fortinet.com/resources/cyberglossary/sextortion (last visited on May 15, 2026).

ISSN: 2582-6433

as offenders may misuse stolen identities for fraudulent activities, illegal transactions, or unauthorized access to systems and services.[11]

5. Child Sexual Abuse Material (CSAM)

Child Sexual Abuse Material (CSAM) refers to any image, video, digital content, or visual representation depicting sexual exploitation, abuse, or sexually explicit activities involving children. The term "CSAM" is increasingly preferred over "child pornography" because it more accurately reflects the abusive and exploitative nature of such material rather than suggesting consent or legality. The creation, possession, distribution, transmission, or viewing of CSAM constitutes a serious violation of children's rights, dignity, and privacy.[12]

6. Online Gaming Exploitation

Online gaming exploitation refers to the misuse of online gaming platforms to manipulate, abuse, or exploit children through cyberbullying, cyber grooming, financial fraud, exposure to harmful content, or unauthorized collection of personal data. Many online games include chat features and interactions with strangers, making children vulnerable to emotional manipulation, harassment, and online predators. Excessive gaming may also expose children to addiction, psychological stress, and privacy risks associated with data tracking and in-game purchases.[13] The rapid growth of multiplayer gaming environments has therefore raised serious concerns regarding child cyber safety and digital privacy.[14]

7. Social Media Manipulation

Social media manipulation refers to the use of digital platforms and algorithmic systems to influence, deceive, or exploit users through misleading content, emotional targeting, behavioural tracking, or psychological pressure. Children are particularly vulnerable to such manipulation due to their frequent use of social networking platforms and limited understanding of online risks. Social media algorithms may expose children to harmful

[11] Fortinet, "Identity Theft", available at: https://www.fortinet.com/resources/cyberglossary/identity-theft (last visited on May 15, 2026).
[12] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women and Children in India* (LexisNexis, New Delhi, 2017) at 172.
[13] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women and Children in India* (LexisNexis, New Delhi, 2017) at 171.
[14] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn., 2022) at 248.

ISSN: 2582-6433

content, misinformation, unrealistic social standards, or addictive digital behaviour, negatively affecting their mental health, privacy, and emotional well-being.[15]The extensive collection of personal data by social media platforms also raises serious concerns regarding children's informational privacy and online safety.[16]

Legal Framework Governing Children's Digital Privacy and Cyber Safety in India

The increasing use of digital platforms by children has raised serious concerns regarding online privacy, cyber safety, and protection against digital exploitation. In India, constitutional provisions, statutory laws, and judicial decisions collectively provide the legal framework for safeguarding children in cyberspace. However, rapid technological advancement and emerging cyber threats continue to challenge the effectiveness of existing laws.[17]

Constitutional Protection of Children's Digital Rights

The Constitution of India guarantees protection of children's dignity, liberty, and privacy through various fundamental rights. Article 21 guarantees the right to life and personal liberty, which has been judicially interpreted to include the right to privacy and informational autonomy. In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court recognized privacy as a fundamental right and emphasized protection of personal data and informational privacy in the digital age.[18] This judgment forms the constitutional basis for protection of children's digital p Article 19(1) (a) guarantees freedom of speech and expression, including expression through digital platforms, while Articles 39(e) and 39(f) direct the State to protect children against exploitation and ensure their healthy development. These constitutional safeguards impose a duty upon the State to establish effective mechanisms for child cyber safety and online protection.[19]

Protection under the Information Technology Act, 2000

The Information Technology Act, 2000 is the principal legislation governing cyber law in India. Section 67B specifically criminalizes publication, transmission, browsing, downloading,

[15] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn., 2022) at 252.
[16] Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing Co., New Delhi, 5th edn., 2016) at 91.
[17] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women and Children in India* (LexisNexis, New Delhi, 2017) at 164.
[18] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[19] Constitution of India, arts. 19(1) (a), 21, 39(e) and 39(f).

ISSN: 2582-6433

or distribution of sexually explicit material involving children in electronic form.[20] The Act also imposes intermediary obligations upon digital platforms and social media companies to remove unlawful content and cooperate with law enforcement authorities.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 further strengthen child online safety by requiring intermediaries to exercise due diligence, establish grievance redressal mechanisms, and prevent circulation of exploitative content. However, challenges relating to enforcement, cross-border cybercrime, and anonymous digital networks continue to hinder effective implementation.[21]

Protection under the POCSO Act, 2012

The Protection of Children from Sexual Offences Act, 2012 provides comprehensive legal protection against sexual offences affecting children, including offences committed through digital platforms. The Act criminalizes online sexual abuse, cyber grooming, child sexual abuse material (CSAM), and exploitation through electronic communication.[22]

The POCSO Act adopts a child-centric approach by providing child-friendly procedures for reporting, investigation, and trial. Courts have repeatedly emphasized that protection of children from digital exploitation must remain a priority in interpretation and enforcement of the Act. Despite its progressive framework, scholars and recent studies have highlighted persistent issues such as underreporting, procedural delays, inadequate victim support systems, and lack of cyber forensic infrastructure.[23]

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a major development in India's data protection framework. The Act contains special provisions relating to children's data protection and requires verifiable parental consent before processing children's personal data. It also restricts behavioural tracking, targeted advertising, and monitoring of children by digital platforms.[24]

The DPDP Act seeks to strengthen informational privacy and accountability in digital environments. However, concerns remain regarding practical implementation, enforcement

[20] *Information Technology Act, 2000*, s. 67B.
[21] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn., 2022) at 245.
[22] *Protection of Children from Sexual Offences Act, 2012*.
[23] Kanchal Gupta and Stuti Pandey, "Protecting Children from Sexual Offences – Challenges and Issues in the Implementation of POCSO Act, 2012" 20 *National Capital Law Journal* 23 (2025).
[24] *Digital Personal Data Protection Act, 2023*.

ISSN: 2582-6433

mechanisms, and balancing privacy protection with technological innovation. Recent academic studies have observed that the increasing use of artificial intelligence and algorithmic systems may create new risks for children's digital privacy and autonomy.[25]

The Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS, 2023), which replaced the Code of Criminal Procedure, modernizes criminal investigation and procedural mechanisms relating to cyber offences and child protection. The BNSS recognizes electronic communication and digital evidence within criminal investigations and permits electronic filing of information relating to cognizable offences under Section 173.[26] The legislation further emphasizes audio-video recording of investigative procedures, electronic communication during investigation, and speedy investigation in offences relating to sexual crimes against children.[27] Section 193 of the BNSS specifically provides that investigation relating to offences under the Protection of Children from Sexual Offences Act, 2012 should ordinarily be completed within two months from recording of information by police authorities.[28] These provisions strengthen procedural efficiency and victim protection in cyber offences involving children.

Juvenile Justice (Care and Protection of Children) Act, 2015

The Juvenile Justice (Care and Protection of Children) Act, 2015 also plays an important role in protecting children affected by online exploitation and cyber abuse. The Act provides mechanisms for care, protection, rehabilitation, counselling, and social reintegration of children who are victims of abuse, trafficking, neglect, or exploitation.[29]Children subjected to cyber grooming, online sexual abuse, trafficking, or digital exploitation maybe treated as "children in need of care and protection" under the Act. The Juvenile Justice framework therefore complements cyber laws by ensuring rehabilitation, psychological support, and institutional care for child victims affected by digital crimes.[30]

[25] Usha Tandon and Neeraj Kumar Gupta, "Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023" 6 *Legal Issues in the Digital Age* 87 (2025).
[26] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 173
[27] Prachi Bhardwaj, "Key Highlights of the Three New Criminal Laws Introduced in 2023", available at: SCC Online Blog (last visited on May 12, 2026).
[28] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 193.
[29] Juvenile Justice (Care and Protection of Children) Act, 2015.
[30] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women and Children in India* (LexisNexis, New Delhi, 2017) at 175.

ISSN: 2582-6433

Judicial Developments Relating to Digital Rights

Indian courts have played an important role in strengthening digital rights and cyber safety protections. In Shreya Singhal v. Union of India, the Supreme Court struck down Section 66A of the Information Technology Act for violating freedom of speech and expression under Article 19(1) (a).[31]The judgment highlighted the need to balance digital freedom with reasonable restrictions aimed at protecting vulnerable users, including children.

Similarly, in Anuradha Bhasin v. Union of India, the Supreme Court recognized the constitutional importance of internet access and digital communication in modern society.[32] These decisions collectively demonstrate the judiciary's evolving approach towards digital rights, privacy, and online protection.

International Framework Governing Children's Digital Privacy and Cyber Safety

Protection of children in digital spaces has become an important concern under international human rights law. Various international conventions, guidelines, and policy frameworks recognize the need to safeguard children from online exploitation, privacy violations, cyber abuse, and harmful digital content while ensuring their right to access information and participate in digital environments.[33]

The most significant international instrument relating to child protection is the United Nations Convention on the Rights of the Child (UNCRC), 1989. The Convention recognizes children's rights to dignity, privacy, protection, development, and access to information. Article 16 protects children against arbitrary or unlawful interference with privacy, while Articles 19 and 34 obligate States to protect children from all forms of abuse, exploitation, and sexual exploitation.[34] These provisions form the foundation for protection of children's digital rights and cyber safety.

The United Nations Committee on the Rights of the Child adopted General Comment No. 25 (2021) on children's rights in relation to the digital environment. The General Comment emphasizes that States must ensure safe digital access for children while protecting them from

[31] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[32] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC
[33] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn., 2022) at 260.
[34] United Nations Convention on the Rights of the Child, 1989, arts. 16, 19 and 34.

ISSN: 2582-6433

cyberbullying, online grooming, data exploitation, and harmful content. It further highlights the responsibility of governments and digital platforms to safeguard children's privacy and personal data in online spaces.[35]

International organizations such as UNICEF and the International Telecommunication Union (ITU) have also developed child online protection guidelines and digital safety initiatives. UNICEF emphasizes child-centred digital policies, privacy protection, and digital literacy to ensure safe participation of children in cyberspace.[36] Similarly, the ITU Child Online Protection framework encourages international cooperation, awareness programs, and stronger cyber safety mechanisms for children.[37]

Regional data protection frameworks have also influenced global standards relating to children's online privacy. The European Union's General Data Protection Regulation (GDPR) contains specific safeguards for children's personal data and requires parental consent for processing children's information below a specified age.[38] Such international frameworks demonstrate the growing recognition of children's digital privacy and cyber safety as essential components of modern human rights protection.

Emerging Technological Threats

1. **Artificial Intelligence and Deepfake Technology**

   Artificial intelligence (AI) and deepfake technology pose serious threats to children's digital privacy and cyber safety. AI-generated images, videos, and audio recordings may be misused for cyberbullying, harassment, and creation of child sexual abuse material (CSAM). Deepfake technology further threatens children's dignity and privacy by enabling creation of manipulated explicit content without consent.[39]

2. **Social Media Algorithms and Data Exploitation**

   Social media platforms use algorithmic systems and behavioural tracking to collect

[35] United Nations Committee on the Rights of the Child, *General Comment No. 25 on Children's Rights in Relation to the Digital Environment* (2021).
[36] UNICEF, "Child Online Protection", available at: https://www.unicef.org/globalinsight/reports/child-online-protection (last visited on May 12, 2026).
[37] International Telecommunication Union, "Child Online Protection", available at: https://www.itu.int/en/cop/Pages/default.aspx (last visited on May 12, 2026).
[38] European Union General Data Protection Regulation, 2016, art. 8.
[39] Usha Tandon and Neeraj Kumar Gupta, "Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023" 6 *Legal Issues in the Digital Age* 87 (2025).

ISSN: 2582-6433

children's personal data for targeted advertising and content recommendations. Such practices raise concerns regarding privacy violations, psychological manipulation, exposure to harmful content, and addictive digital behaviour affecting children's mental health and well-being.[40]

3. **Online Gaming and Encrypted Platforms**

Online gaming platforms expose children to cyber grooming, cyberbullying, financial fraud, and interaction with anonymous users.[41] Similarly, encrypted communication systems and anonymous digital networks create challenges for investigating cyber offences and circulation of exploitative material involving children.[42]

4. **Educational Technological Platforms and Privacy Risks**

Educational technology platforms often collect children's personal and behavioural data without adequate privacy safeguards. Inadequate regulation of such platforms may lead to unauthorized data sharing, profiling, and commercial exploitation of children's information.[43]

Socio-Legal Challenges in Protecting Children's Digital Privacy and Cyber Safety.

1. **Lack of Digital Awareness**

One of the major challenges in protecting children online is the lack of digital literacy among children, parents, and teachers. Many children are unaware of cyber risks such as cyberbullying, online grooming, privacy violations, and identity theft. Similarly, parents and educational institutions often lack adequate knowledge regarding safe digital practices and online supervision.[44]

2. **Underreporting of Cyber Offences**

Cyber offences against children are frequently underreported due to fear, social stigma, emotional trauma, and lack of awareness regarding legal remedies. Victims and families

[40] Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing Co., New Delhi, 5th edn., 2016) at 91.
[41] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women and Children in India* (LexisNexis, New Delhi, 2017) at 171.
[42] Talat Fatema, *Cyber Crimes* (Eastern Book Company, Lucknow, 2016) at 118.
[43] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn., 2022) at 252.
[44] Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing Co., New Delhi, 5th edn., 2016) at 87.

ISSN: 2582-6433

often hesitate to approach law enforcement authorities, resulting in many cases of online exploitation remaining hidden and unaddressed.[45]

3. **Weak Enforcement Mechanisms**

Although India has enacted laws such as the Information Technology Act, 2000 and the Protection of Children from Sexual Offences Act, 2012, effective implementation remains a challenge. Many law enforcement agencies lack adequate cyber forensic infrastructure, technical expertise, and specialized training required for investigation of digital offences involving children.[46]

4. **Technological Advancement and Emerging Threats**

Rapid technological development has created new forms of cyber threats including artificial intelligence-generated exploitation, deepfake technology, encrypted communication systems, and anonymous online networks. Existing legal frameworks often struggle to address these evolving technologies and cross-border cybercrimes effectively.[47]

5. **Privacy versus Surveillance Concerns**

Protection of children online often requires monitoring and regulation of digital activities. However, excessive state surveillance and data monitoring may conflict with the constitutional right to privacy recognized in Justice K.S. Puttaswamy v. Union of India. Balancing child protection with privacy and digital freedom therefore remains a significant socio-legal challenge.[48]

6. **Commercial Exploitation of Children's Data**

Social media companies, gaming platforms, and EdTech applications frequently collect and process children's personal data for advertising and commercial purposes. Inadequate transparency and weak consent mechanisms increase the risk of data misuse, profiling, and behavioural manipulation of children in digital spaces.[49]

[45] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women and Children in India* (LexisNexis, New Delhi, 2017) at 176.
[46] Talat Fatema, *Cyber Crimes* (Eastern Book Company, Lucknow, 2016) at 121.
[47] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn., 2022) at 245.
[48] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[49] *Digital Personal Data Protection Act, 2023*.

ISSN: 2582-6433

7. **Jurisdictional and Cross-Border Issues**

   Cyber offences often involve offenders operating across different states or countries, making investigation and prosecution difficult. Jurisdictional complexities, anonymous digital identities, and lack of international cooperation frequently delay effective legal action against cyber offenders targeting children.[50]

Critical Analysis

India has developed a significant legal framework for protection of children's digital privacy and cyber safety through constitutional safeguards, the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, the Juvenile Justice Act, and the Digital Personal Data Protection Act, 2023. These laws collectively recognize the importance of protecting children from online exploitation, cyber abuse, and privacy violations.[51] Judicial decisions such as Justice K.S. Puttaswamy v. Union of India have further strengthened the constitutional recognition of informational privacy and digital rights.[52]

Despite these developments, several limitations continue to affect effective implementation. Weak cybercrime investigation mechanisms, lack of technological expertise, underreporting of offences, and inadequate digital awareness among children and parents reduce the practical effectiveness of legal protections.[53] Existing laws also struggle to address emerging technological threats such as artificial intelligence-generated exploitation, deepfake technology, encrypted platforms, and cross-border cybercrime.[54]Moreover, social media companies and digital platforms continue extensive collection and commercialization of children's personal data, raising concerns regarding informed consent and behavioural manipulation.[55]

Therefore, although India has established an evolving legal framework for child cyber safety, stronger enforcement mechanisms, child-centric digital policies, cyber awareness programs,

[50] Usha Tandon and Neeraj Kumar Gupta, "Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023" 6 *Legal Issues in the Digital Age* 87 (2025).
[51] Debarati Halder and K. Jaishankar, *Cyber Crimes against Women and Children in India* (LexisNexis, New Delhi, 2017) at 164.
[52] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[53] Talat Fatema, *Cyber Crimes* (Eastern Book Company, Lucknow, 2016) at 121.
[54] Chris Reed, *Internet Law* (Cambridge University Press, Cambridge, 9th edn., 2022) at 245.
[55]Usha Tandon and Neeraj Kumar Gupta, "Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023" 6 *Legal Issues in the Digital Age* 87 (2025).

ISSN: 2582-6433

and international cooperation are necessary to ensure effective protection of children's rights in digital spaces.

Conclusion

Children's digital privacy and cyber safety have emerged as critical socio-legal concerns in the contemporary digital age, as increased use of social media, online gaming, educational platforms, and digital communication systems has exposed children to cyberbullying, online grooming, identity theft, data exploitation, and child sexual abuse material. India has established an evolving legal framework through constitutional protections, the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, the Juvenile Justice Act, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, while judicial decisions such as Justice K.S. Puttaswamy v. Union of India have strengthened the constitutional recognition of privacy and informational autonomy. Nevertheless, rapid technological advancement, emerging threats such as artificial intelligence-generated exploitation and deepfake technology, weak enforcement mechanisms, underreporting of cyber offences, and lack of digital awareness continue to challenge effective child protection in cyberspace. Therefore, ensuring a safe digital environment for children requires stronger implementation of laws, child-centric cyber policies, digital literacy, parental supervision, institutional accountability, and international cooperation to safeguard children's dignity, privacy, development, and overall well-being in the digital era.

IJLRA