



Digital Childhood at Risk: A Doctrinal Analysis of Online Abuse and Child Protection Laws in India

Subhadra Hansda, Dr. Parimita Dash

Research Scholar, Associate Professor

KIIT University

Abstract

The swift development of digital technologies has transformed the way children relate to cyberspace but increased their exposure to cyberbullying, cyber exploitation and digital victimisation. This article aims to discuss the adequacy of Indian legislative framework to ensure the online safety of children with a specific reference to the constitutional provisions, Protection of Children from Sexual Offences Act, 2012, Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023. The research is based on doctrinal and comparative methods. It considers the context of the statute, common law and international norms set out in the United Nations Convention on the Rights of the Child and current digital safety regimes in the European Union and United Kingdom. The essay argues that the current Indian framework is fragmented and not sufficient to deal with evolving issues such as intermediary liability, encrypted communication, AI-generated exploitative content and cross-border cybercrime. It also “highlights child-centric digital governance, enforcement gaps and institutional collaboration.” The study observes that India needs a holistic, technology-responsive legal framework based on constitutional values and principles of child rights and a greater degree of regulatory accountability for effective protection of children in digital spaces.

KEYWORDS: Child Rights, Online Abuse, Cyber Exploitation, Digital Safety, Child Protection, Cybercrime, POCSO Act, Intermediary Liability, Artificial Intelligence

1. INTRODUCTION

The rapid integration of digital technologies into the daily lives of children has changed the way children interact, communicate, learn and socialise, while also exposing children to new forms of online abuse and cyber exploitation. Online abuse covers abuse, cyberbullying, grooming, sextortion, doxing, exposure to harmful content and sharing of personal information without consent on digital platforms. Cyber exploitation also includes the use of technology to facilitate sexual, psychological or economic abuse, including via Child Sexual Abuse Material (CSAM), online trafficking and exploitative activities on social media, gaming platforms, encrypted apps and anonymous forums. Digital victimisation differs from traditional abuse as it is

anonymous, permanent, rapidly spreading, transnational and causes children ongoing psychological, emotional and reputational harm.

The digital damage has increased with the technological development and the algorithmic systems. The anonymity of cyberspace provides an opportunity for criminals to conceal their identity and abuse children by setting up fake profiles and providing false information. End-to-end encryption is a significant challenge to privacy and data security, but also a challenge for law enforcement agencies to detect and investigate online exploitation. Furthermore, the emergence of deepfakes, synthetic exploitative imagery and AI-assisted grooming has exposed important gaps in existing legal systems and increased the risk of the use of artificial intelligence technologies. What this means is that there is a technologically mediated ecosystem of child exploitation that is transnational and transcends traditional criminal methodologies. Social media and recommendation engines use algorithms that amplify harmful content and accelerate the spread of abuse. Children are particularly vulnerable in digital environments, a fact which is even more evident due to developmental, psychological, educational and socio-economic factors. Younger users might be less mature and less able to understand manipulative behaviour or judge risks online, making them vulnerable to grooming, coercion and exploitation. Psychological vulnerabilities like loneliness, anxiety and need for social acceptance, increase exposure to negative interactions further. This is further compounded by the low digital literacy, poor parental supervision and lack of awareness on privacy and cybersecurity. In cyberspace, children are more vulnerable because of socio-economic inequalities, disability, migration, displacement and gender-based discrimination. Child protection in the digital space, therefore, means child-friendly laws, better regulation, digital literacy and technology-sensitive policies that can bring together innovation, privacy and child protection.

Digital technologies are evolving at a rapid pace and have played a key role in reshaping childhood, introducing the internet, social media, online games and AI-powered platforms into children's everyday lives. "Digitalisation provides new opportunities for communication, learning and social participation, but it has also exposed children to new forms of online harm. Cyber grooming, sextortion, cyberbullying, revenge pornography, online trafficking, identity theft, deepfake exploitation and the circulation of child sexual abuse material (CSAM) have emerged as serious threats to online environments. The use of artificial intelligence, encrypted communication systems and algorithmic platforms has further increased the vulnerability of children in cyberspace. Internationally, the United Nations Convention on the Rights of the Child requires States to protect children from all forms of exploitation. Whereas in India, there are constitutional guarantees and legislations such as the Protection of Children from Sexual Offences Act, 2012 and Information Technology Act, 2000, to regulate online harms to children. But India faces serious doctrinal and regulatory challenges in dealing with children's cyber exploitation. The current body of law is piecemeal and incapable of regulating new technologies like AI-generated exploitative content and deepfake abuse. The lack of effective enforcement mechanisms, institutional lapses in cyber policing and the absence of comprehensive legislation on child online safety hamper effective protection further. Tensions over digital surveillance make it difficult to craft rules that both protect children and preserve constitutional rights to privacy and free expression. The study therefore adopts a doctrinal and comparative approach to critically examine the

constitutional provisions, statutory frameworks, judicial decisions and international legal standards on child online safety. The research aims to study the legal frameworks in other jurisdictions such as European Union, United Kingdom and Australia to compare intermediary liability and to identify the gaps in Indian law and suggest reforms to improve the digital protection mechanism for children.

2. INTERNATIONAL LEGAL FRAMEWORK ON DIGITAL SAFETY OF CHILDREN

The United Nations Convention on the Rights of the Child (UNCRC) is the most important international instrument protecting the rights of children, including their rights in digital environments. While the Convention was adopted before the widespread use of the Internet, its principles are increasingly being applied to cyberspace and digital governance. In all actions concerning children, including in digital policies and in the regulation of online platforms, the ‘best interests of the child’ shall be a primary consideration, in line with Article 3 of the UNCRC. Article 16 Right of the child to privacy and protection against arbitrary or unlawful interference with his or her personal data, communications and online identity. Article 19 requires States to protect children from all forms of violence, abuse, neglect and exploitation, which now includes cyberbullying, online grooming, digital harassment and other forms of online abuse. Article 34 also mandates States to take measures to prevent child sexual exploitation, including online child sexual abuse and trafficking and exploitation facilitated by digital platforms.

In this respect, a significant development has been the General Comment No. 25 of the UN Committee on the Rights of the Child (2021) concerning children’s rights in the digital environment. The General Comment underlines the importance of safe access to the internet, protection from harmful content online, digital literacy, privacy safeguards and the accountability of governments and technology companies. It recognises that digital technologies provide wonderful opportunities for children’s education, development and participation, but also pose serious online risks for children if not properly regulated. In addition to the UNCRC framework, a number of other international instruments and guidelines are available to support the protection of children in digital environments. The Budapest Convention on Cybercrime promotes international cooperation to combat cyber crimes such as online child pornography and cyber exploitation. The Lanzarote Convention also deals with the protection of children from sexual exploitation and abuse through the use of digital technologies and online communication systems. UNICEF has also prepared guidance notes on child online safety, digital literacy, responsible use of technology and protection of children’s privacy in cyberspace. The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography further strengthens the obligation of States to criminalise trafficking, sexual exploitation and child pornography, including offences committed through the use of internet-based technologies.

Together, these international frameworks provide important global benchmarks for the protection of children online. One of the guiding principles is the “best interests of the child” in that all laws, policies, technologies and regulatory systems should prioritise the safety, dignity and well-being of children. Another key principle is the recognition of the developing capacities of children, such that digital regulation and protections are age appropriate and responsive to the developmental maturity of children. The idea of “digital dignity” is about protecting children from online exploitation, invasive surveillance, privacy violations and unsafe digital

behaviours that put their identity and mental health at risk. The standards are built on a child-centric approach to governance and they require governments, schools, technology companies and civil society organizations to develop digital policies and online platforms that prioritize children's rights and safety.

3. CONSTITUTIONAL AND STATUTORY FRAMEWORK IN INDIA

The legal framework for the protection of children from online abuse and cyber exploitation in India is provided in the constitutional and statutory provisions. The Indian Constitution recognises a set of fundamental rights that relate to the protection of children in digital spaces. Article 21 guarantees the right to life, and personal liberty and the Supreme Court has interpreted it broadly to include dignity, privacy, safety, mental health and protection from exploitation. Article 21 Violations of the dignity and psychological security of the child, abuse in cyberspace, cyberbullying, sexual exploitation and circulation of harmful digital content "Article 21A, also speaks about the right to free and compulsory education to children in the age group of six to fourteen years. The growing reliance of modern education on digital platforms and online learning systems makes it necessary to create a safe digital environment for the effective realisation of educational rights. Article 14 provides for equality before law and equal protection of laws and therefore requires equal protection of all children from digital crimes irrespective of their gender, caste, disability or socio-economic background. The State is empowered to make special provisions for children under Article 15(3), and the Constitution also lends support to child-specific laws and welfare measures in cyberspace. In addition, the Directive Principles of State Policy contained in Articles 39(e), 39(f) and 45 of the Constitution of India direct the State to protect children from exploitation and to ensure their healthy development, care and education.

The Protection of Children from Sexual Offences Act, 2012, is the principal law for addressing online sexual exploitation of children. 13. Sections 13 to 15 make child pornography, possession or distribution of child sexual abuse material (CSAM) and electronic transmission of exploitative content involving children criminal offences. The Act acknowledges that children may be targeted and exploited through social networking sites, digital platforms and electronic communications systems. It also includes publication, storage and dissemination of abusive content through online platforms and computer systems. There are, however, serious evidentiary challenges to enforcing these provisions, such as encrypted communications, cross-border cyber offences, anonymous offenders and challenges in collecting and authenticating digital evidence in courts.

The Information Technology Act, 2000, also governs cyber offences and intermediary liability. Section 66E: Non-consensual capture and sharing of private images Section 67B: Child pornography, online child abuse and viewing or downloading of sexually explicit content involving children. Section 69A gives the government the power to prevent the dissemination of information on the internet that is detrimental to the public or children. Intermediaries such as social media platforms are entitled to "safe harbour" protection under section 79 if they meet certain due diligence requirements and remove unlawful content when notified. "If an intermediary knowingly hosts child abuse material, or fails to remove illegal content or fails in their duty to protect children, they can be held liable under the law." Digital platforms should therefore work with law enforcement agencies, establish grievance redressal mechanisms and follow government guidelines on online child protection.

The Juvenile Justice (Care and Protection of Children) Act, 2015, also has significance in the welfare of children affected by cyber exploitation, trafficking, online abuse and digital victimisation. The Act defines victims as “children requiring care and protection” and provides for rehabilitation and counselling, institutional support and social reintegration. The Digital Personal Data Protection Act, 2023, also seeks to safeguard the privacy and personal data of children in digital spaces. The Act obliges online platforms to obtain verifiable parental consent before processing children’s data, and to limit harmful profiling, behavioural tracking and targeted advertising of minors. However, these protections remain widespread as there are major regulatory gaps, weak monitoring systems, a lack of digital awareness, vague standards of implementation and a lack of accountability of global technology companies. There are no specific rules under the existing architecture on emerging tech harms, such as exploitative content generated by AI, algorithmic harms to children in digital spaces and deepfakes.

4. JUDICIAL INTERPRETATION OF CHILD PROTECTION ONLINE

Indian courts are increasingly acknowledging the need for special protection for children in digital spaces, while balancing such protection with constitutional rights such as privacy and freedom of speech. The judiciary has recognised that Article 21 of the Constitution includes the right to privacy, dignity and mental well-being of children, but it has also accepted that reasonable restrictions may be imposed for investigating cyber abuse, online grooming, child pornography and other forms of digital exploitation. The courts have reaffirmed the government’s authority to block websites and online content that contains Child Sexual Abuse Material (CSAM) under the Information Technology Act, 2000, in order to prevent the dissemination of harmful material involving children. Trends in the judiciary have also been increasingly emphasising the responsibility of social media platforms and intermediaries to remove harmful content and report illegal activities, cooperate with investigations and exercise due diligence to protect children from exploitation online. The courts have also cautioned that excessive censorship could violate the freedom of speech and expression under Article 19(1)(a). Therefore, the restrictions on online content must satisfy the tests of legality, necessity and proportionality.

However, there are still considerable procedural and evidentiary barriers to effective enforcement against online child exploitation. End-to-end encryption in digital platforms makes it difficult to access child abuse images and other electronic evidence. “Criminals often hide behind fake accounts, VPNs and anonymous platforms, which makes it difficult to detect and prosecute,” he said. Jurisdictional issues add another layer of complexity to investigations, as cybercrimes are frequently transnational, with victims, offenders and digital platforms located in different countries. International cooperation is therefore essential but often hindered by the different legal systems and procedural requirements in investigation and prosecution. There are also serious problems of doctrinal inconsistencies and implementation that plague the Indian legal system. There are many laws like Protection of Children from Sexual Offences Act, 2012, Information Technology Act, 2000 and the Juvenile Justice (Care and Protection of Children) Act, 2015 with overlapping provisions on online child protection causing confusion in interpretation and implementation. There is also poor coordination between police authorities, cybercrime units, child welfare agencies and intermediaries. The

point is that India does not have a comprehensive and holistic digital child protection law that addresses online child safety, AI generated exploitative content, platform accountability and emerging technological risks. The current framework is therefore fragmented, reactive and inadequate to address rapidly evolving forms of cyber-exploitation of children.

5. INTERMEDIARY LIABILITY AND PLATFORM RESPONSIBILITY

Meta, Google, and X Corp are key players in how children experience the digital world. According to Indian cyber law, intermediaries have to take reasonable care to stop the spread of harmful or illegal content about children. This obligation involves monitoring for illegal content, processing complaints, collaborating with law enforcement agencies and ensuring compliance with standards for child safety. The “notice-and-takedown” regime obliges digital platforms to remove illegal content, including Child Sexual Abuse Material (CSAM), when they are put on actual notice or obtain actual knowledge of such content. Intermediaries may incur legal liability if they fail to act within a reasonable time. Algorithmic systems such as recommendation engines, targeted advertising and auto-suggestion tools have exacerbated concerns around online child safety in recent years, as these systems can unintentionally promote exploitative or harmful material. Hence, digital platforms should ensure their technological systems and algorithms do not aid online exploitation or victimisation of children.

Intermediary liability: Under Section 79 of the Information Technology Act, 2000, social media platforms are not liable for third-party content if they act as intermediaries, follow due diligence requirements, and expeditiously remove illegal content when notified. But platforms can be held liable if they knowingly host illegal activities or fail to remove harmful content related to child exploitation. Indian courts have been increasingly stressing that intermediaries should take proactive steps towards compliance measures and expedite content removal processes in cases of online child abuse and CSAM. Section 79 is an attempt to find the middle ground between freedom of digital communication and the need to protect children from online harm. Digital child protection is a big challenge as it seeks to find the balance between privacy rights and online safety and surveillance measures. End-to-end encryption helps keep private communications private and confidential by blocking unauthorised access. Strong encryption can also hamper law enforcement agencies from detecting online grooming, trafficking or the circulation of exploitative content involving children. So, the governments want more powers of surveillance to investigate such crimes. But privacy activists argue that excessive surveillance may violate the fundamental right to privacy under Article 21 of the Constitution of India. The proportionality doctrine is employed in Indian constitutional jurisprudence. It states that any limitation on the right to privacy must have a legitimate aim, be necessary in a democratic society and be proportionate to the objective sought to be attained. Children’s protection in cyberspace should therefore be carefully balanced with individual privacy rights and digital freedoms. Emerging technologies and artificial intelligence have made the issues of online child protection even more complex. Even where there is no actual child involved physically, AI-generated deepfakes and synthetic sexual imagery can produce false exploitative content involving minors. Such digitally manipulated content can lead to serious psychological and reputational damage and also poses complex legal questions, as existing laws were passed

before the advent of generative AI technologies. Grooming, exploitation and abusive interactions with children can also be made more possible by artificial intelligence systems, recommendation algorithms, chatbots, and anonymous digital networks. There are no specific provisions in the Indian legal framework at present to deal with AI-generated child sexual abuse material and technology-assisted exploitation. This underscores the urgent need for improved child protection laws that are specific to technology.

6. COMPARATIVE ANALYSIS

One of the most developed legal systems for the protection of children in the digital environment has been developed by the European Union. The Digital Services Act (DSA) sets binding obligations on online platforms to protect users, in particular minors, from harmful and illegal digital content. Major social media companies need to swiftly take down unlawful content, assess the risks and be open about their algorithms and online advertising. “The DSA is a preventative law, so platforms have to deal with risks to children in a preventative way and not reactively once harm is done. The General Data Protection Regulation (GDPR) strengthens the protection of children’s personal data by emphasising the need for parental consent, limiting profiling and targeted advertising to minors, and classifying children as a vulnerable data subject requiring special protection. It also discusses platform accountability, data protection, child-centred digital governance and forward-looking regulation. The key advantage is that it creates positive legal obligations for intermediaries, rather than criminal sanctions after the abuse has occurred. 2023 Online Safety Bill: “The UK is very tight on regulation. The Act places a statutory duty of care on digital platforms to protect children from harmful online content, including pornography, cyberbullying, self-harm material, grooming and exploitative content. That gives the Office of Communications (Ofcom) the power to regulate online platforms and fine them if they don’t play ball. It needs better content-filtering and age-verification systems to protect children from harmful content. The UK approach has the advantage of framing online safety as a regulatory issue, rather than a personal responsibility issue, making tech companies, rather than individual users, accountable.

Australia has also taken a specialist, institutionally oriented approach, e.g. the eSafety Commissioner model, one of the most successful child online safety systems in the world. The eSafety Commissioner is Australia’s independent online safety regulator and has the authority to receive complaints, order the removal of harmful content, investigate cyber abuse and promote digital literacy initiatives. The Australian framework is not just about punishment, but also about quick response mechanisms, victim support services, preventative education and inter-agency co-ordination. The big plus is that it creates a separate body just for digital safety and online harms.

India needs an all-encompassing and integrated framework on child online safety and not the current siloed approach where protections are spread across various laws such as the Information Technology Act, 2000; Protection of Children from Sexual Offences Act, 2012 and Juvenile Justice (Care and Protection of Children) Act, 2015. Second, India can build on the example of the European Union and the United Kingdom to create stronger intermediary accountability mechanisms. This could be done by making social media companies identify, monitor and prevent harmful content from reaching children in the first place. Third, the Australian experience shows the importance of a dedicated and independent digital safety regulator to respond quickly

to online harms and support victims effectively. However, wholesale adoption of foreign regulatory models may not be entirely appropriate in the Indian context, due to issues like digital illiteracy, limited cyber infrastructure, resource constraints, federal administrative complexities and constitutional issues relating to privacy and freedom of speech. Therefore, India needs a nuanced and calibrated legal framework that strikes a balance between the need for child protection and the constitutional protections. India's legal framework for protecting children online has structural and practical shortcomings. The law's fractured and that is one of the big problems." There are many statutes on online child abuse and cyber exploitation, which adds to the redundancy and interpretive ambiguity. At present, there is no one overarching digital child protection law, which results in uneven enforcement and implementation of policies. The other big problem is weak institutions, weak enforcement. Cybercrime units are often under-resourced, with poorly trained staff and limited high-level technological expertise and digital forensic infrastructure to investigate sophisticated offences that use encrypted exploitation networks, anonymous platforms and AI-generated abusive content. Moreover, the legal framework is largely punitive, and lacks sufficient mechanisms for the rehabilitation of victims, psychological counselling, social reintegration and long term support to the affected children. Moreover, India lacks the technological capability to combat emerging threats such as deepfakes, synthetic child sexual abuse material and AI-enabled exploitation, especially since most of the existing laws were enacted prior to the advent of advanced generative artificial intelligence technologies. Children, parents and educators lack mechanisms for digital literacy and low awareness of online risks, reporting procedures and cyber safety practices making them more vulnerable to exploitation.

The Indian approach is more reactive rather than preventive in character. The focus is on punishment after the damage has been done, rather than creating strong preventive systems through accountability of the platforms, technological regulation, digital education and specialised institutional oversight. Hence, there is an immediate need for a child-centric digital safety framework which includes constitutional rights, governance of technology, accountability of intermediaries, rehabilitation of victims and prevention through regulatory mechanisms for effective child protection in the digital spaces.

7. RECOMMENDATIONS AND REFORM PROPOSALS

India needs a more robust, coordinated and comprehensive legal framework to protect children in the digital space. Current laws are patchwork and often fail to keep up with new online threats such as cyber grooming, exploitative content created by AI, deepfakes and online trafficking. We have to legislate specifically for the regulation of online harms against children with a comprehensive Child Online Safety law.

There is also a need to bring in AI specific legal provisions to criminalise the creation and dissemination of AI-generated child sexual abuse material and digitally manipulated exploitative content. Social media platforms and intermediaries should be subject to higher standards of accountability, including faster removal of harmful content, mandatory reporting requirements and stronger due diligence mechanisms. Governments should set up dedicated cyber child protection units with trained investigators and digital forensic experts to tackle online child exploitation effectively. Since cyber offences have trans-border implications, India must step up international cooperation and information-sharing arrangements with foreign agencies and

international organisations. The school curriculum should also include education on digital literacy and online safety to help children, parents and teachers to recognise and deal with risks online. It said there was a need for child-friendly reporting systems and psychological support services for victims to report and receive rehabilitation. Finally, we could establish an independent digital safety regulator to enforce compliance, child protection standards and accountability of digital platforms.

8. CONCLUSION

The fast development of digital technology has changed childhood profoundly, opening up new possibilities for education, communication and social participation. However, it has also posed a serious threat of online abuse, cyber exploitation and digital victimisation to children. India has a plethora of laws to protect children, but the legal framework remains fragmented, reactive, and insufficient to meet emerging technology threats. Thus, a rights-based and techno-sensitive approach is necessary for effective protection of children in digital environments. We need stronger laws, institutional reforms, platform accountability and international cooperation to protect the dignity, privacy and well-being of children in cyberspace. The protection of children in the digital environment is not a cyber regulation issue only. It is an issue of constitutional and human rights, and it is fundamental for the preservation of childhood, dignity and human development in the digital age.

REFERENCES

International Instruments

United Nations. (1989). Convention on the Rights of the Child. United Nations.

United Nations. (2000). Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. United Nations.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Budapest.

Council of Europe. (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Lanzarote.

United Nations Children's Fund. (2020). Child Online Safety: Global Challenges and Strategies. UNICEF Publications.

United Nations Committee on the Rights of the Child. (2021). General Comment No. 25 on Children's Rights in Relation to the Digital Environment. United Nations.

Indian Legislations

Constitution of India. (1950). Government of India.

Information Technology Act, 2000. (2000). Government of India.

Protection of Children from Sexual Offences Act, 2012. (2012). Government of India.

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

Digital Personal Data Protection Act, 2023. (2023). Government of India.

Books and Reports

Basu, D. D. (2021). Introduction to the Constitution of India (26th ed.). LexisNexis.

Kaushal, K. (2022). Cyber Laws and Information Technology. Central Law Publications.

Nappinai, N. S. (2019). Technology Laws Decoded. LexisNexis.

United Nations Office on Drugs and Crime. (2021). Study on Online Child Exploitation and Abuse. UNODC Publications.

Internet Watch Foundation. (2023). Annual Report on Child Sexual Abuse Material Online. IWF Publications.

Journal Articles

Bhatia, G. (2020). Privacy, surveillance and constitutionalism in India. National Law School of India Review, 32(2), 45–67.

Kumar, V. (2021). Online child sexual exploitation and legal responses in India. Indian Journal of Law and Technology, 17(1), 89–112.

Mitra, A. (2022). Intermediary liability and child protection in cyberspace. Journal of Cyber Policy, 7(3), 233–248.

Sharma, R. (2023). Artificial intelligence and child safety: Emerging legal concerns in India. International Journal of Law and Information Technology, 31(2), 120–139.

Foreign Legislations and Regulatory Frameworks

European Union. (2022). Digital Services Act. European Parliament.

European Union. (2018). General Data Protection Regulation (GDPR). European Parliament.

United Kingdom. (2023). Online Safety Act. Parliament of the United Kingdom.

Australia. (2021). Online Safety Act. Commonwealth of Australia.