YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

The Dark Side of the Internet: Cyber-Crime Against Children and the Law

Aditya Bisen, B.A.LL.B, School of Law, Lovely Professional University

Published on: 6th September 2025

Abstract

Children now have a plethora of educational, social, and informational options because to the digital revolution. They now face significant dangers of cybercrime, too, as a result of the same technical improvements. Children are especially susceptible to risks including cyberbullying, online grooming, child pornography, dark web trafficking, and identity theft because of their psychological immaturity, curiosity, and reliance on online platforms. The scope and complexity of these offences have increased due to adolescents' growing use of digital devices and social media.

Protections against the online exploitation of kids are provided in India by laws like the Protection of Children from Sexual Offences (POCSO) Act, 2012, and the Information Technology Act, 2000, which are complemented by the Juvenile Justice Act, 2015. International agreements such as the United Nations Convention on the Rights of the Child (UNCRC) and the Budapest Convention[8] on Cybercrime highlight the need of states to safeguard children online. To evaluate the efficacy of legal solutions, this article uses a doctrinal and analytical approach, looking at legislative provisions, court rulings, and comparative international frameworks.

The study finds that although there are laws to prevent cybercrime against minors, their implementation is still very difficult because of jurisdictional complications, online anonymity, and low levels of cyber literacy among stakeholders. To guarantee a safer online environment for kids, it ends by suggesting a multifaceted strategy that includes improved legislative protections, technology safeguards, digital literacy initiatives, and international collaboration.

KEYWORDS: *Cyber-crime against children; Online child exploitation; Cyberbullying; Online grooming; POCSO Act; Information Technology Act; UNCRC.*

INTRODUCTION

One of the biggest problems of the digital age is cybercrime, which includes a variety of illegal actions conducted via computers, networks, and online platforms. It is more difficult to identify and prosecute than traditional crimes since it is anonymous and spans national borders. Such offences have a significantly greater detrimental effect on children as they jeopardise not only their immediate safety but also their long-term development and psychological health.

Children are particularly at danger in cyberspace because of their inability to comprehend hazards, innate propensity for trust, and extensive exposure to digital technology. Their susceptibility to risks including identity theft, online grooming, cyberbullying, and exposure to pornography has increased due to their increased dependence on cell-phones, social media, and online learning platforms. Children and parents that lack digital literacy make this vulnerability even more vulnerable, which makes it easier for them to be exploited.

Recent reports provide insight into the scope of the problem. According to UNICEF, one in five people who use the Internet have encountered unsolicited sexual solicitations, and one in three Internet users worldwide are children. The National Crime Records Bureau [1](NCRB) in India has documented a steady growth in cybercrimes committed by children, with particular rises in offences under the categories of child pornography and online harassment. These figures highlight how urgent it is to review the legislative and policy structures designed to safeguard children online.

Although India has specialised laws, such as the Information Technology Act of 2000 and the Protection of Children from Sexual Offences (POCSO) Act of 2012, there are still enforcement loopholes. Problems including cross-border jurisdiction, quick technical advancements, and the anonymity of offenders make it more difficult for current rules to be effective.

This study aims to address these issues by examining the types of cybercrimes against children, assessing how well India's legal system works, and making comparisons with other international agreements like the Budapest Convention on Cybercrime[2] and the United Nations Convention on the Rights of the Child. Additionally, the study seeks to suggest legislative, policy, and educational initiatives that might improve children's online safety and promote a safer online environment.

RESEARCH METHODOLOGY

This study looks at the legal and policy aspects of cybercrimes against minors using a doctrinal and analytical approach. The research assesses the advantages and disadvantages of the existing legal

[1] Nat'l Crime Records Bureau, *Crime in India* (latest report), Ministry of Home Affairs, India.
[2] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998).

system by concentrating on statute provisions, court rulings, and academic discussion. While the analytical technique enables a critical evaluation of how these laws react to changing digital dangers, the doctrinal method is suitable in this situation since it makes it easier to comprehend current rules in detail and apply them practically.

Legislative measures like the Protection of Children from Sexual Offences Act of 2012, the Information Technology Act of 2000, and the Juvenile Justice (Care and Protection of Children) Act of 2015[3], as well as important court rulings on the online exploitation of minors, are primary sources of information. These are complemented by secondary sources, such as scholarly works, National Crime Records Bureau records, and global publications from agencies like UNICEF.

The study also uses a comparative lens to place India's reaction in a larger context by looking at certain foreign legal systems and international treaties[4] like the United Nations Convention on the Rights of the Child and the Budapest Convention on Cybercrime. This makes it possible to comprehend international best practices holistically and how they relate to India's initiatives to protect children online.

FORMS OF CYBER-CRIMES AGAINST CHILDREN

With its educational, socialising, and recreational potential, the Internet has become an essential element of children's life. On the other hand, it has also made them more vulnerable to various cybercrimes that take advantage of their weaknesses. Although these offences differ in type and severity, they all have detrimental effects on children's physical, mental, and emotional health.

Cyberbullying, which includes harassment via digital platforms like social media, messaging apps, and online gaming forums, is one of the most prevalent types. Children who are humiliated, threatened, or excluded online frequently suffer from anxiety, sadness, and in extreme situations, suicide thoughts. According to UNICEF reports, cyberbullying is incredibly common, with almost one in three youth worldwide having been victims of some kind of it.

Another issue is internet grooming, in which predators build trust with children through extended online communication with the goal of sexually exploiting them. Frequently, grooming occurs in chat rooms, gaming networks, or social networking sites, where victims are tricked into disclosing private information or graphic pictures. The Protection of Children from Sexual Offences (POCSO) Act in India is seeing a rise in cases involving online grooming, exposing how predators take advantage of the anonymity of the internet.

[3] Juvenile Justice (Care and Protection of Children) Act, No. 2, Acts of Parliament, (2015) (India).
[4] United Nations Convention on the Rights of the Child, art. 34, Nov. 20, 1989, 1577 U.N.T.S. 3 [hereinafter UNCRC].

Child pornography is still one of the most dangerous online crimes that target minors. This encompasses the creation, ownership, dissemination, and dissemination of sexually exploitative material involving children. The Information Technology Act of 2000's Section 67B expressly makes such offences illegal. Online service providers are held accountable in the historic **Avnish Bajaj v. State (Bazee.com case)**[5], when an intermediate platform was found accountable for the dissemination of child-related pornographic content. According to NCRB data, child pornography-related cybercrimes in India have increased significantly in recent years, frequently thanks to encrypted platforms.

Dark web exploitation and cyber trafficking have also become much more of a threat. In secret internet networks, traffickers are increasingly using bitcoin payments and encrypted communication to promote or trade child sexual abuse material (CSAM). Due to the dark web's covert nature, it is difficult to uncover and prosecute cases, leaving minors open to worldwide exploitation.

Financial fraud and identity theft involving children are also growing issues. Children regularly divulge personal information online, which makes it easy for their identities to be used for fraudulent transactions or the construction of false accounts. These offences, albeit being less obvious, can have a lasting impact on a child's digital imprint and financial stability.

All of these types of cybercrimes highlight how urgently strong security measures are needed. Each category shows how technology may be abused in a variety of ways and highlights how traditional law enforcement is unable to combat technologically advanced and transnational crimes. It takes a mix of robust legislative frameworks, cutting-edge cyber-forensic technologies, and awareness campaigns to address these hazards, enabling kids, parents, and educators to identify and react to online threats.

INDIAN LEGAL FRAMEWORK

The legal system in India has worked to provide responses to the increasing problem of cybercrimes against minors. Targeted legislation, cyber law[6] revisions, rehabilitation statutes, and updated criminal law provisions make up this framework. Court rulings have also influenced the practical application of these rules, demonstrating the courts' recognition of children's vulnerability in the digital age.

The Protection of Children from Sexual Offences Act, 2012[7]

Protecting children from sexual abuse, especially crimes made possible by internet platforms, is primarily accomplished by the Protection of Children from Sexual Offences (POCSO) Act, 2012. The

[5] Avnish Bajaj v. State, Crim. M.W.P. No. 753/2003, Delhi High Court (India).
[6] Information Technology Act, No. 21, Acts of Parliament, (2000) (amended 2008) (India).
[7] Protection of Children from Sexual Offences Act, No. 32, Acts of Parliament, (2012) (India).

exploitation of minors to produce or disseminate pornographic content is particularly illegal, and it acknowledges the dangers of cyberstalking and online grooming. In-camera procedures, obligatory reporting, and victim identity protection are just a few of the Act's noteworthy child-centric aspects. POCSO exhibits legislative foresight by addressing online forms of exploitation, so guaranteeing that children are protected from growing kinds of abuse and adjusting to technologies.

The Information Technology Act, 2000 (as amended in 2008)

India's fundamental legislative foundation for controlling online behaviour is provided by the Information Technology Act, 2000. Its applicability in shielding kids from online abuse was greatly increased by the 2008 amendment. Minors are disproportionately targeted in privacy crimes, and Section 66E makes it illegal to take or send pictures without permission. Even more crucial is Section 67B, which forbids the production, distribution, or viewing of anything that shows youngsters engaging in sexually explicit behaviour. Importantly, this clause also holds other parties accountable, including social media sites and Internet service providers, for wilfully permitting the spread of such information. By requiring platforms to answer, the legislation acknowledges that internet is a communal environment in which accountability goes beyond the direct offender.

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

The Juvenile Justice Act of 2015, despite its wider reach, is essential in resolving the fallout from cybercrimes against children. This Act provides for the care and rehabilitation of children who are victims of cyber exploitation, internet pornography, or human trafficking. Through measures like special juvenile police units and Child Welfare Committees, the Act guarantees victims long-term protection, reintegration, and counselling. It is a crucial addition to the legal response to juvenile cybercrime because it places more of an emphasis on rehabilitation than punishment, setting it apart from existing legislation.[8]

The Bharatiya Nyaya Sanhita, 2023

The criminal law system in India has seen a substantial change with the passage of the Bharatiya Nyaya Sanhita (BNS), 2023[9]. Provisions pertaining to child exploitation, sexual assault, and trafficking are preserved and reinforced in the Act. Even while its prohibitions aren't just focused on cybercrimes, they do interact with the IT Act and POCSO when online behaviour crosses over into more conventional crimes like sexual harassment or slavery. By bringing traditional criminal laws into line with modern digital issues, the BNS therefore serves as a harmonising force.

[8] Juvenile Justice (Care and Protection of Children) Act, No. 2, Acts of Parliament, (2015) (India).
[9] Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).

Judicial Perspectives

When it comes to interpreting and implementing these rules in the digital realm, court rulings have been essential. In Avnish Bajaj v. State, sometimes referred to as the Bazee.com case, the Delhi High Court considered an intermediate platform's culpability when it allowed the dissemination of pornographic content involving children. The case made it clear that intermediaries need to keep a close eye on their platforms to stop these kinds of abuses and cannot claim total immunity. Another significant ruling was Shreya Singhal v. Union of India[10], in which the Supreme Court upheld the necessity of controlling harmful internet information while also invalidating Section 66A of the IT Act on the basis of free expression. The court's understanding of striking a balance between basic rights and the state's obligation to safeguard vulnerable populations, especially minors, online is reflected in the ruling.

An Integrated Approach

All of these laws and court rulings work together to create a multi-tiered framework for preventing cybercrimes against minors in India. The IT Act deals with electronic transmissions, the POCSO Act makes online exploitation a direct crime, the Juvenile Justice Act offers rehabilitation assistance, and the Bharatiya Nyaya Sanhita strengthens the penalties. Judicial actions also guarantee accountability in a changing digital landscape. Nevertheless, issues including uneven enforcement, cross-border jurisdiction, and technical anonymity still restrict efficacy. Collaboration with technology providers, improved investigation capabilities, and judicial sensitivity are all necessary to address these problems in addition to stricter legislation.

INTERNATIONAL LEGAL FRAMEWORK

Because cybercrimes are typically multinational in scope, safeguarding minors from online exploitation transcends national borders. International legal documents and comparative laws from other jurisdictions show the shortcomings in India's present framework and offer insightful information about best practices.

United Nations Convention on the Rights of the Child, 1989

The United Nations Convention on the Rights of the Child (UNCRC) continues to be the most important international agreement pertaining to parental rights. Article 36 expands the duty of States Parties to prohibit additional types of exploitation that can jeopardise the wellbeing of children, while Article 34 requires them to protect children from all forms of sexual exploitation and abuse. According to a wide interpretation of these clauses, the digital world is included, guaranteeing that states take

[10] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

action to shield kids from trafficking, pornography, and online grooming.[11]

Budapest Convention on Cybercrime, 2001

The first global agreement to tackle cybercrime through standardised legislation, investigative methods, and international collaboration is the Budapest Convention. Because of the global nature of the Internet, its provisions specifically criminalise child pornography and stress the necessity of cross-border cooperation in investigations. India has not, however, ratified the Convention due to issues with jurisdiction and sovereignty. Due to its non-ratification, India has been unable to fully engage in organised international collaboration, which has made it more difficult to combat cybercrimes that start or spread across national borders.

U.S. Children's Online Privacy Protection Act, 1998

Protecting children under 13's privacy online is the goal of the groundbreaking Children's Online Privacy Protection Act[9] (COPPA) in the United States. It requires parental approval before gathering, using, or sharing a minor's personal information online. COPPA acts as a model for protecting children's privacy, an area in which Indian legislation is constantly evolving, especially when it comes to social media and educational platforms that frequently collect personal data about children.

U.K. Sexual Offences Act, 2003

Modern types of sexual exploitation, such as grooming, are covered by the UK's Sexual Offences Act[12]. In particular, setting up a meeting with a youngster after communicating with them online with the goal of sexually exploiting them is illegal. By acknowledging grooming as a separate crime, the law offers a powerful deterrent against child exploitation made possible by online platforms.

Comparative Assessment

India has implemented robust internal regulations like the IT Act and POCSO, but its inability to participate in treaties like the Budapest Convention limits its capacity to successfully collaborate in cross-border investigations, as can be seen by comparing these international frameworks. India would be much better equipped to safeguard children online if it included aspects of international best practices, especially in the areas of data protection and grooming regulations.

JUDICIAL RESPONSE IN INDIA

In India, judicial interpretation has played a significant role in defining the parameters of cybercrime legislation, especially with regard to safeguarding children online. Throughout history, courts have

[11] United Nations Convention on the Rights of the Child, art. 34,36, Nov. 20, 1989, 1577 U.N.T.S. 3 [hereinafter UNCRC].
[12] Sexual Offences Act, 2003, c. 42 (U.K.).

stressed the necessity to strike a balance between the advancement of technology and basic rights and the need to protect vulnerable populations, including children.

Recognition of Intermediary Liability

Avnish Bajaj v. State[5], sometimes referred to as the Bazee.com case, is a seminal ruling in this regard. In it, the Delhi High Court considered the culpability of an internet platform for hosting pornographic content involving children. The case demonstrated that middlemen must check material carefully and cannot avoid accountability by only serving as facilitators. The judiciary's determination to make digital intermediaries responsible for protecting minors from online exploitation was emphasised by this ruling.

Balancing Freedom of Expression and Child Protection

In Shreya Singhal v. Union of India[6], the Supreme Court's decision further honed the legal discussion around Internet governance. In addition to highlighting the state's obligation to control harmful internet information, the Court invalidated Section 66A of the Information Technology Act for being ambiguous and overbroad in limiting free expression. Judicial sensitivity to the conflicting demands of protecting minors from harmful and exploitative online information and allowing them to express themselves freely is evident in the ruling.

Evolving Judicial Sensitivity

A rising judicial understanding of the particular vulnerabilities that children confront in the digital age has been shown by subsequent opinions. Given the necessity of taking preventative action against child pornography, cyberbullying, and online grooming, courts have placed a greater emphasis on child-centric interpretations of laws such as the POCSO Act and IT Act. While putting the child's best interests first, this changing judicial approach shows an attempt to modify conventional legal thinking to the difficulties of internet.

CHALLENGES IN ENFORCEMENT

The complicated and dynamic nature of digital offences makes it difficult to execute laws against cybercrime directed at minors, which goes well beyond legal prohibitions.

Jurisdictional Complexities: Cross-Border Barriers

When crimes occur in different countries, jurisdictional limits provide a significant challenge to the prosecution of cyber offences against children. Because the Internet has no geographical boundaries, criminals frequently take advantage of this by targeting victims from outside their own country or storing illicit information on servers located in other countries. Such transnational crimes necessitate coordinated responses from law enforcement organisations throughout the globe, but international cooperation systems and mutual legal assistance treaties (MLATs) are frequently sluggish and

expensive. These delays make it more difficult to respond quickly, which occasionally enables criminals to avoid punishment or destroy important evidence.

Anonymity and Encryption: The Challenge of the Dark Web

Offenders are now able to conceal their identities and activities thanks to the development of online privacy technologies and the growth of encrypted platforms. Investigators find it extremely challenging to follow transactions, identify the people disseminating child sexual abuse materials, or trace origins due to the usage of cryptocurrencies, the dark web, and end-to-end encryption techniques. Such investigations frequently require a level of technological skill that is beyond the existing capabilities of law enforcement, enabling criminals to camouflage themselves behind many layers of digital technology.

Digital Illiteracy: Vulnerabilities and Victimization

Insufficient awareness of cyber hazards, proper online conduct, and the strategies used by thieves to prey on the weak is a problem for many kids, their parents, and even teachers. Young victims are more vulnerable to online harassment, frauds, and grooming because of this lack of digital literacy, which frequently leaves them ignorant of their rights and accessible resources for help. Because awareness efforts and digital safety education are still in their infancy in many areas, exploitation rates are greater and abuse is less likely to be detected.

Stigma and Underreporting: Obstacles to Justice

When it comes to online sexual exploitation, harassment, or bullying, social shame and cultural taboos deter children and their families from reporting violations to the police. Many people underreport because they are afraid of being blamed, shunned, or having their reputation damaged. This leaves trauma untreated and gives offenders more confidence. Digital surroundings can make it difficult for victims to express their experiences, which makes case discovery and investigation much more difficult.

Deficit in Specialized Enforcement: Need for Trained Cyber Police

The actual execution of legal measures that recognise the dangers of cyberspace to children is hindered by a shortage of qualified staff with expertise in online criminal investigation and cyber forensics. Many police departments struggle to respond quickly to complex crimes because they lack the necessary technology tools and knowledge. The needs set by the changing digital threat landscape cannot yet be met by investments in specialised cybercrime units, frequent training, and sophisticated analytical tools.

These complex issues highlight the pressing need for more flexible tactics, global cooperation, increased digital literacy, and funding for specialised enforcement systems in order to successfully address the problem of cybercrime against minors.

PREVENTIVE & POLICY MEASURES

Empowering Young Internet Users through Education

Reducing the threats that children face online requires the expansion of digital education programs. Cyber safety modules that are included into school curricula provide pupils the skills they need to identify suspicious activity, navigate digital settings safely, and comprehend the repercussions of disclosing personal information. To ensure that adults can successfully counsel children and react quickly to internet risks, these programs should also include parents and teachers.

Building Multi-Sector Networks for Child Safety

Government agencies, tech companies, and non-governmental organisations must work together to actively protect children online. To improve content moderation practices and quickly handle child exploitation cases, regulatory bodies must collaborate with social media companies and internet service providers. While coordinated efforts may dismantle silos and provide a comprehensive strategy to child online protection, NGOs play a crucial role by providing victim care, increasing public awareness, and pushing for legislation reform.

Advancing Investigative Capabilities

Improving training and infrastructure for cyber forensics is essential for efficient law enforcement. Advanced analytical tools and ongoing capacity-building initiatives should be funded by agencies so that police can find, save, and interpret digital evidence of abuse. By showing that they are technologically prepared, specialised cybercrime units devoted to child exploitation cases promote effective investigations and discourage criminal activity.

Making Child Reporting Simple and Accessible

The protection of children depends on having access to secure, easy-to-use platforms for reporting online crimes. Reporting procedures must to be made as easy as possible, provide multilingual assistance, and reduce fear. Guidance via chat rooms or helplines gives victims more self-assurance, promotes prompt action, and lessens their fear of shame or retaliation.

Responsible Guardianship: Privacy and Oversight

Respecting children's autonomy while maintaining monitoring must be carefully balanced for parental engagement to be effective. Even if monitoring software and parental controls offer protections, too much intervention might erode a child's confidence or obstruct sincere connection. To ensure that children are proactive agents in their own digital safety while simultaneously getting watchful care from guardians, families should prioritise open communication, establish limits, and foster trust.

These actions create a robust ecosystem that actively protects children from cyberthreats while upholding their rights and dignity when incorporated into national policy and community activity.

CONCLUSION

In today's digitally linked world, the frequency of cybercrime directed against children poses serious concerns to their safety, mental health, and future development. Such crime is a crucial problem. Although India has extensive regulatory frameworks, such as the Information Technology Act, the POCSO Act, and recent legislative revisions, enforcement is still uneven and sometimes ineffectual. Technology complexity, resource limitations, and regulatory loopholes prevent these laws from reaching their full protective potential.

To tackle this complex issue, a comprehensive strategy involving strong collaboration amongst several stakeholders' government organisations, tech firms, civil society groups, educators, and families—is needed. The only way to improve enforcement, put creative safety measures in place, and increase victim rehabilitation programs is to work together.

Additionally, it is crucial to prioritise ongoing education and awareness in order to equip kids and carers with the knowledge and abilities necessary to securely traverse the digital world. At the same time, it is essential to periodically update laws to reflect technological developments in order to plug present gaps and foresee new dangers. Public awareness initiatives are essential for shattering taboos and promoting prompt reporting of violations.

In conclusion, establishing a safer online space for kids necessitates consistent dedication from all facets of society. India can gradually protect its younger generation from the negative aspects of cyberspace and uphold their right to a safe and encouraging digital future by integrating legal strictness, technical alertness, community involvement, and educational programs.

REFERENCES

1. Protection of Children from Sexual Offences Act, No. 32, Acts of Parliament, (2012) (India).
2. Information Technology Act, No. 21, Acts of Parliament, (2000) (amended 2008) (India).
3. Juvenile Justice (Care and Protection of Children) Act, No. 2, Acts of Parliament, (2015) (India).
4. Bharatiya Nyaya Sanhita Act, 2023 (India).
5. Avnish Bajaj v. State, Crim. M.W.P. No. 753/2003, Delhi High Court (India).
6. Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012, Supreme Court of India.
7. United Nations Convention on the Rights of the Child, art. 34, Nov. 20, 1989, 1577 U.N.T.S. 3 [hereinafter UNCRC].
8. Budapest Convention on Cybercrime, Nov. 23, 2001, 2242 U.N.T.S. 145.
9. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998).
10. Sexual Offences Act, 2003, c. 42 (U.K.).
11. Nat'l Crime Records Bureau, *Crime in India* (latest report), Ministry of Home Affairs, India.
12. UNICEF, *Child Online Safety and Protection: Global Status Report* (2023).
13. United Nations Office on Drugs and Crime, *The Impact of Cybercrime on Children: International Perspectives* (2022).
14. M. Cherif Bassiouni, International Cooperation in Cybercrime Investigations, 15 J. Int'l Crim. Just. 233 (2017).