

Online child safety and legal protections in India – (cyberbullying, online sexual exploitation, laws and enforcement)

Prakhar Mishra¹, Vaishnavi Singh² and Dr. Sneha Tiwari³

^{1,2} LLM Student, Uttar Pradesh State Institute of Forensic Science, Lucknow

³ Assistant Professor, Uttar Pradesh State Institute of Forensic Science, Lucknow

Abstract—The fast growth of internet accessibility in India has greatly marked children's involvement with online platforms leading to both advantages and disadvantages. This article explores inspect risks to child safety online especially cyberbullying and online sexual exploitation, which have arisen as notable issues in the digital era. Cyberbullying impacts children's mental health resulting in anxiety, depression and social isolation while online sexual exploitation subjects minors to grooming, abuse and trafficking dangers.

The research also examines the legal structure in India intended to safeguard children in the online environment. Key legislations like the Information Technology Act, 2000 and the Protection of Children from Sexual Offences (POCSO) Act ,2012 along with sections of the Indian Penal Code which tackles different types of online harassment. Government efforts such as cybercrime reporting platforms and educational campaigns, significantly contribute to prevention and response.

Notwithstanding of these actions hurdles keep on in successful enforcement because of underreporting, insufficient digital literacy, jurisdictional complications for law enforcement agencies. The article underlines the necessity for better enforcement of regulations, improved team work among parties involved and increased digital education for children, guardian and teachers. Ensuring the safety of children online in India necessitates a extensive strategy that integrates legal, technological, and social measure.

Index Terms—Children, Cyberbullying Cybercrime, Protection, , Technology.

I. INTRODUCTION

The digital revolution has altered childhood in India since education, entertainment, socialising, etc, have never been more accessible than it is now. Nevertheless, this access is becoming more dangerous due to identity theft, sexual exploitation on the Internet, cyberbullying, as well as access to content harmful to well-being. India boasts of one of the largest child populations in the entire world, in which the number of children below the age of 18 exceeds 5 hundred million. It has significant challenges in ensuring Child online safety. Geared towards awareness creation, the association between technology and child vulnerability prompts the need to have a comprehensive legal reaction grounded on digital ethics and rights safeguard. What exacerbates this problem further is the unique social and economic components in India, such as the diverse systems of the devices that are utilised by individuals, including both basic and advanced knowledge on the utilisation of technology, disproportional distribution of available tools that enable the safety of children on social networks and other tools that they can utilise. The laws and organisations, which are supposed to protect children online in India, are evolving, yet they are not united entirely, and, in most cases, they take action only when something negative takes place, not prior to it. This is what makes the use of digital means allow people to remain anonymous and ensure that their activities will last indefinitely, and since bad people are incredibly intelligent, they take advantage of this in numerous online locations by inviting children in very clever fashions. It has seen the hazards, and India

has already passed valuable laws such as the Information Technology Act⁴ the Protection of Children from Sexual Offences Act⁵ and the Digital Personal Data Protection Act⁶. The laws that exist are meant to address various dimensions of online risks. Additionally, enforcers such as the National Commission for Protection of Child Rights and special groups dealing with cyber safety are responsible for enforcing the laws and supporting victims. Yet, there are still some enforcement issues in the area, such as confusing applicability, not enough special consideration and protective guidance for children, and new risks like using AI to deceive or harm children, which complicate the possibility of the duty to protect knowing concepts of the law.

II. DIGITAL RISKS FACED BY CHILDREN IN INDIA

Many online threats and harms present risks to children in India due to their lack of knowledge about staying safe online, and the fact that they are disproportionately engaged with digital tools. Children can become victims of cyberbullying - to be bullied, threatened or hurt online through social media and messaging apps is common and hurts children's well-being and mental health. There is also a risk of an existing case in relation to online sexual exploitation where individuals attempt to persuade children to disclose private information, share dark content or provide personal information to facilitate future sexual exploitation. Children are also at risk of having their personal data hijacked for unknown purposes and being disengaged from children, leading to risks of identity theft or tracking.

Cyberbullying is a major risk today when children regularly get bullied, threatened or made to feel bad through social media, messaging apps or online groups. Cyberbullying also appears to negatively affect children's mental health, leading to thoughts of self-harm, anxiety, sadness, or simply feeling bad about oneself. The way this affects children shows how important it is to have strong laws and support

systems in place. Online sexual exploitation is also a serious problem. Others attempt to lure children into chatting with them on the internet, and this may result in sexual assault, the dissemination of unlawful materials, or even putting them in direct physical harm. It has been reported that this form of online abuse has only intensified, particularly in the pandemic, when kids were spending more time online due to home-based school and less outdoor time.

III. CYBERBULLYING AND HARM

One of the most common online risks to children is cyberbullying. It can manifest in many different forms, like doxing, defamation, and mockery, and it is commonly carried out via social media, messaging apps, and gaming platforms. Research has connected cyberbullying to anxiety, depression, and, in extreme situations, like youth suicide or self-harm. This concerning trend was reflected in the (NCRB)⁷ report 2023, which showed a 25% increase in cybercrimes related towards minors.

The Information Technology Act, 2000 give provision to fight for online harassment under Sections 66A⁸ and 67, which are mostly general. Enforcement remains inconsistent due to a lack of apprehension and specialised training for cyber cells and other cyber departments. The prevention of cyber crimes against women and children (CCPWC) program provides some relief by spreading awareness and response to the sectors. However, like international laws such as the UK Online Safety Act The India does not yet have any specific kind of law that focuses only on cyberbullying among minors.

IV. IMPACT OF CYBERBULLYING

Cyberbullying can gravely harm an individual's feelings and mental state in ways that last for a long period. People who are bullied online frequently feel very sad and scared, and feel very poor about themselves. They may even have feelings of worthlessness and deep emotional distress. This

⁴ Information technology Act, 2000 ,No.21 of 2000, India.

⁵ Protection of children from sexual offences Act,2012, No.32 of 2012, India.

⁶ Digital personal data protection Act,2023, No.22 of 2023 , India.

⁷ National Crime Records Bureau's

⁸ Information technology Act,2000,§ 66A, No. 21 of 2000, India

emotional suffering can produce its own physical suffering, leading to headaches, stomach pain, trouble sleeping, and even muscular tension. New research nowadays shows that the strain of cyberbullying can lead to emotional distress so acute that some children think about self-harm or injure themselves, pointing out the serious nature of online bullying.

In addition, these impacts are especially harmful to children since they could hinder their ability to build friendships or perform academically. Children who are amenable to bullying online often have difficulty focusing or concentrating, have declining performance in school, and may even choose not to engage on the internet altogether. This establishes a cycle of increasing loneliness and academic difficulties.

Online sexual exploitation: Fixing

Online sexual exploitation is one of the serious online crimes against children. Criminals exploit minors through delusive grooming, coercion, and child sexual abuse. The Protection of Children from sexual Offences (POCSO) Act, 2012 criminalised both physical and sexual virtual abuse, targeting actions such as child pornography and virtual grooming. Further the Section 67B⁹ of the Information Technology Act, 2000 directly prohibits the announcement or circulation of sexually explicit content that involves children and is punishable by imprisonment (rigorous).

India has set up technical agencies like the Ministry of Home Affairs Online Child Sexual Abuse and Exploitation Prevention Unit (OCSAE) to deal with OSE cases. The Cyber Tipline Report System, in collaboration with Interpol and NCPCR which allows citizens to report cases related to online child sexual exploitation. Despite these measures, even today, underreporting is still common because of stigma and fear among the victims and the complexity of the technicalities of tracking offenders as they tend to have multiple jurisdictions spread.

Most disturbing of all is the live-streaming of sexual abuse, a new dimension of exploitation. The extant IT laws in India criminalise the transmission of offensive material but do not address the live streaming of such

abuses or the deployment of emerging technologies that create synthetic sexual content involving minors such as deepfakes. The gap in legislation enables offenders to act with near impunity. Urgent reform is needed to provide for specific punishment for these fast-evolving methods of online sexual exploitation.

Online sex trafficking is a critical problem, which Indian law criminalises in the recruitment, harbouring, and exploitation that happens through coercion or deception. It remains difficult to enforce, however, when the exploitation occurs behind encrypted networks or crosses state or national borders, and many of these cases use cryptocurrency and the dark web. Victims often face coercion not only directly online but also through threats leveraging intimate images-a phenomenon variously known as sextortion, currently encoded as a separate offence in India.

Legal Framework and Constitutional Protections

The digital safety of children in India was based on several laws. According to the Information Technology (IT) Act, 2000 service providers of online services should exercise the precaution and erase any content that would lead to any harm. (DPDPA)¹⁰ offers a greater safeguard by ensuring that the companies obtain the consent of a parent that can be verified prior to their accessing a child with the use of his or her personal information, as stipulated by Article 9. It is punitive to individuals who violate the regulations and holds digital platforms accountable. The Companies are also ordered according to the IT (Intermediate Guidelines and Digital Media Ethics Code) 2021, to prevent children from accessing harmful or otherwise inappropriate not good for them.

According to K.S. Puttaswamy¹¹ judgment, the concept of privacy as a fundamental right has been provided under the Indian Constitution Article 21 that digital child protection has a foundation in the Constitution. The plans, such as the national cyber security policy (2013), the INSPIRE framework, the national children policy (2013), as well as supporting these laws by giving them safe online spaces, by teaching, prevention, and positive quick actions.

⁹ Information technology Act, 2000, § 67B, No. 21 of 2000, India.

¹⁰ The Digital Personal Data Protection Act 2023.

¹¹ Justice K.S. Puttaswamy v. union of India (2017) 10 scc1.

Government Initiatives and Policy Measures

The Digital Personal Data Protection Act 2023 is significant. The act has amended that talks of seeking parental consent before information on children can be used by platforms. It also avoids profiling children of the companies, which is also good for data privacy. This has been assisted by the Ministry of Electronics and Information Technology, known as Minitiy, which has recently come out with guidelines to support this legislation. These new rules address the limitations of AI-generated content, as well as making platforms more accountable. They are enclosed in the 2021 Intermediary Guidelines.

One more thing is the Digital India Act, which will reverse the entire picture of the interaction with the sphere of cyberspace. This will involve disclosure of algorithms, faster content moderation posts, more safeguards for children on the internet, and more physical punishment for those who commit acts of violence against children.

The public policies that are being developed under the INSPIRE framework are focused primarily on the safety of children. Some of the focuses are on online safety, online education, online mental health, and promoting positive social interaction and behaviour.

Role of NGOs and Civil Society

In India, non-governmental organisations are key players in developing safe online spaces for children. They help children who have experienced online abuse to report the cyber abuse. They also help in securing counselling and legal services for child victims of online exploitation.

The organisations often collaborate with the government to suggest that they must more vigorously enforce laws, be more flexible and protective. They also give enlightenment programs to kids and parents, and teachers, so that all the people are enlightened on the potential harm that can be done online. The organisations work in partnership with the government, parents and the technology companies so as to come up with meaningful digital literacy and encourage the use of the internet safely and responsibly.

Comparative Perspective and Global Benchmarks

The legislation of India, when analysed in the scope of the rest of the world, demonstrates a lot of similarities, yet cannot be compared to the power of the legislation concerning children in the European Union and the US. As an example, in the US, we have the Children Online Privacy Protection Act (COPPA), which outlines regulatory provisions on online security which is not entirely covered in the existing legislation in India. India will have to develop more robust and unified legislation directed to child safety, which will bring it close to the global standards and enforce those laws.

Some of these attributes are reflected in a specific strategy on safety towards children by potentially prohibiting violent, self-harming and pornographic content on the Australian Online Safety Act, and other industry laws regulating hosting service providers, added in or around 2025. The law puts finer demands on platforms to provide adequate reporting and takedown systems and engagement processes, in addition to restricting children's access to otherwise unsafe content. Australia is recognised nationally for creating specific government entities, including the Safety Commissioner, which is intended to enforce age and content regulation.

China has also acted to impose strict rules around digital content aimed at minors, including proposed rules for categorising online content that affects children's bodily and mental well-being. This also brings limits on the duration of games for younger users, bans on accessing violent or pornographic material, and restrictions to regulate and address compulsive engagement with the online activity. Perhaps with a more central and regulative model, this indicates an increasing awareness of safeguarding minors' wellbeing in more rapidly digitalising societies.

Judicial Interpretations and Key Cases

Indian courts are beginning to realise that online crimes against children are distinct from regular crimes, and to amending laws to ensure online conduct such as grooming and cyber harassment fall under their existing child protection laws.

V. LANDMARK CASES AND THEIR IMPACT

1. Shreya Singhal v. Union of India

This case¹² has special importance about free speech and online abuse. The Supreme Court struck down Section 66A of the Information Technology Act. The current provision criminalised merely sending offensive messages online, said the provision's definition of offensive messages was impermissibly vague and broad in relation to the right of free speech under Article 19(1)(a).

In addition to this move protecting fundamental rights, it also served as a line to limit the government's intrusion into online speech. The result of such a ruling has been more significant and more lucrative in the regulatory actions towards online speech that enhance the regulation of management standards that are equitable.

2. Sabu Mathew George v. Union of India

The Supreme Court of this case¹³ dealt with internet harassment and the content found on the internet that spread gender discrimination. The Court ordered that businesses, including Google, Yahoo and social media firms, need to make efforts to block the spread of content that promotes illegal actions (e.g., illegal gender determination) that breach the PCPNDT Act. The Court urged companies to participate in activities that may prevent the sharing of illegal and harmful content and increased the clarity of the fact that digital companies have a responsibility to prevent online abuse and bullying.

3. Kalandi Charan Lenka v. State of Odisha (2017)

The case¹⁴ concerning the establishment of fake accounts on social media and promotion of indecent content surrounded the violation of the dignity and privacy of the victim.

The Odisha High Court affirmed the accusations against these offences in terms of Section 66C and 67 of the IT Act, that abusing the platform maliciously and with intent to harass and defame others was a violation of the law. In this instance, the court affirmed that users and social media platforms must take due

diligence in preventing and controlling any harm that might follow the occurrence of cyberbullying, especially in false profiles and defamation.

VI. LANDMARK CASE LAW RELATED TO ONLINE SEXUAL EXPLOITATION IN INDIA

The Indian courts have already started to directly address the issues of online child sexual exploitation with significant decisions that not only derive meaning within the already existing laws, but also give further and broader legal protection as established in laws like the Protection of Children against Sexual Offences Act (POCSO Act) and the Information Technology (IT) Act.

An example of one such case and also one of the landmark cases is the matter of J.B. Pardiwala and Chief Justice D.Y. Chandrachud in the Supreme Court case Just Rights for Children Alliance vs. S. Harish [2024] that specifically covers the issue of distance, online exploitation of a child.

The case was initiated when the Madras High Court declared that the possession of child sexual abuse material was not a crime in itself, and this posed a great challenge to whether the law was capable of addressing the new social danger to children. The Supreme Court reversed the decision and explained that not only the seeing, possessing, and having appeared as a crime according to Section 15 of the POCSO Act, but also Section 67B of the IT Act. The reasoning of the Court in the decision itself was victimization oriented and included the redefinition of a child pornography under a more narrow term, Child Sexual Exploitative and Abuse Material (CSEAM); the criminalization of just having such material, no intent to transmit; the enforcement of an obligation on the intermediaries like social media and hosts to report and delete such material as soon as possible; and alignment of India with the demands of the United Nations Convention on the Rights of the Child (UNCRC) to a greater degree. The Court noted that such exploitation of children online colonises their dignity and right to life under Article 21 of the

¹² Shreya Singhal v. Union of India, AIR 2015 SC 1523.

¹³ Sabu Mathew George v. Union of India, (2018) 3 SCC 229.

¹⁴ Kalandi Charan Lenka v. state of Odisha, BLAPL No. 7596 of 2016, Orissa High court.

Constitution, and would recommend additional legislation to enhance child protection.

One more important case is Sabu Mathew George v. Union of India (2017), where the Supreme Court ruled that intermediaries needed to go out of their way to censor the contents that they transmit to avoid the transmission of illegal content that facilitates sexual exploitation. This case became a precedent of holding the digital platforms accountable for their obligation to safeguard children on the internet. In the case of S. Harish ¹⁵, the Madras High Court in the early case resulted in a storm of legal cases by saying that child pornography should be demonstrated as distributed to be a crime, later subdued by the Supreme Court in the previously mentioned case. It was done after the Supreme Court made a ruling in response to that, to enable the execution of more stringent interpretations of laws on child protection as per the international standards.

The Role and Function of the Supreme Court in Increasing

The courts have emphasised how social media companies ought to take an active part in controlling and policing the toxic nature of the content on their sites.

They have, in reality, proposed that such firms need to keep on checking and deleting harmful content. These companies have also received more responsibility over the protection of their users by the courts, and this has been given more weight in protecting the vulnerable users of the company, such as women and children. They are also expected to help the police and other authorities in developing a safer internet environment in the Supreme Court in Extending Protection.

Judicial Opinions about Free Speech and Online Harassment

Courts are indeed appreciating the importance of free speech and, at the same time, attempting to limit online harassment and bullying. In the significant case Shreya Singhal v. Union of India, the court said the limitation of the freedom of speech of citizens online should be fair, intelligible and not excessive in a way that we would be depriving the citizens of their fundamental entitlements arbitrarily. The court went ahead to say

that citizens were free to express their views which may be inflammatory or offensive but not too much as to restrain meaningful conversation of other citizens. However, the legislation is allowed and ought to intervene when an individual masquerades as another person, propagates hatred or otherwise runs or misuses or dominates another person.

Enforcement and Its Challenges

The intentions of the legislative practices in India are strong, but the trauma related to implementation remains a problem. In this case, numerous law enforcement agencies would not possess the cyber forensics competencies to address the sophisticated offences like deepfakes and misuse of encrypted communications. These platforms do not necessarily provide modern design codes and rational content moderation, and this is not achieved without explicit duties of the roles in the IT rules. The proposed Digital India Act (DIA), intended to supersede the IT Act, is aimed at eliminating these problems, or the absence thereof, through adding algorithmic accountability, age-appropriate design, and more stringent platform responsibilities. There are also socio-cultural challenges regarding these perils; parents' awareness of the digital platforms remains low at the time. Further, there has been a recent trend in creating awareness of the concern, such as the recommendation by MeitY ¹⁶ to address AI-generated threat data, and the Child Online Safety Declaration 2025 established by Kerala, which shows that people are beginning to perceive this as a problem. This all needs a firm implementation both at the governmental level and to enhance the collaborative efforts of the governments with the technology companies of the private sector and the civil societies. Deepfakes represent risk in terms of sexual exploitation and to creation of synthetically based scams, as well as algorithmic feeds potentially exposing minors to harmful content. The recently introduced Digital India Act is expected to regulate such threats by implementing age restrictions, data localisation and content tracking mechanisms, along with putting onus on respective intermediaries to be accountable for unintended amplification of such content and represents a first step towards reformative modernisation of cyber laws in India.

¹⁵ 2020

¹⁶ Ministry of Electronics and information Technology.

VII. RECOMMENDATIONS FOR A SAFER DIGITAL CHILDHOOD

1. Mandate an age verification mechanism with a privacy-friendly design to prevent identity misuse in the digital field.
2. Should provide advanced training for law enforcement in digital forensics and victim-sensitive response.
3. Provide a Public awareness campaign on digital literacy and responsible use of technology among parents and educators.
4. Collaboration of multi-stakeholders with governments and their agencies, NGOs and platforms to develop child-centric design norms.
5. Expansion of POCSO's digital reach to cover evolving technologies such as AI-generated imagery and social engineering.
6. Develop Child-Safe Technological Tools.
7. laws to explicitly criminalise new forms of digital abuse, such as sextortion, live-streaming of abuse, AI-generated deepfakes, and enforce stricter penalties for offenders.
8. Support families and educational institutions to support outdoor play, movement and hobbies in addition to limited screen time to assist with alternative development and to decrease screen time.
9. Update existing laws to clearly criminalise new forms of digital abuse, such as sextortion, live-streamed abusive acts, and AI-generated deepfakes and impose stronger consequences for offenders.

VIII. CONCLUSION

Online child safety in India is at a critical point. The more deeply children are involved in digital ecosystems, the more a balance between protection and autonomy becomes a constitutional and ethical imperative for states. The currently existing regulatory frameworks, like the IT Act, POCSO and DPDPA, offer the much-needed protection, but they need to be enforced in more gradual and immediate ways in India. The government is needed not only to enforce laws rigidly against all predominantly in this regard but also to induce a cultural transformation that favours digital awareness, understanding and accountability throughout the entire society. Only in

terms of the strategy of inclusiveness can India be guaranteed that the opportunities of technology will not be imposed on the youngest citizens of the country, but will be used to their advantage.

India has succeeded in establishing a comprehensive legal framework, which brings the Information Technology Act, the Protection of Children from sexual offences (POCSO) Act and the Digital Personal Data Protection Act into a holistic framework, which presents a viable platform instead of the protection of children on the Internet. The emergence of groundbreaking cases, especially by the Supreme Court, has caused an upsurge in India in its fight against the Child Sexual Exploitative and Abuse Material (CSEAM) and, currently, even, criminalisation of possessing and viewing CSEAM. The courts also established the mediator liability, platform accountability, a stainless guard of victim dignity and privacy that modelled the legal rationale in various circumstances with regard to technology.

REFERENCE

Books -

- [1] IT Act, 2000
- [2] Digital Personal Data Protection Act, 2023
- [3] Protection of Children from sexual Offences Act, 2012

Websites –

- [4] <https://www.wikipedia.org>
- [5] <https://blog.ipleaders.in>