



The Legal Landscape of Cyberbullying and Social Media Privacy: Challenges and Opportunities to Protect Children

Adithya Manikandan
1st Year BBA LLB (Hons.)

Abstract

The increasing presence of children in social media platforms raise concerns for their personal safety, privacy and overall well-being. As many children are exposed to social media, they are indeed exposed to risks such as exploitation, cyberbullying and privacy violations. Additionally, the vulnerability of them is also tested by poor parental guidance and lack of awareness. The legal systems lack specific provisions to govern Cyber bullying and digital privacy crimes. In spite of living provisions in national and international legal bodies, there exist a gap between implementation of these provisions from paper to reality, mainly concerned with enforcement and safeguarding children's data from being misused. This article explores the challenges faced by children in the digital world, stressing on the negative impacts of harmful and faked content, peer pressure, and excessive use of social media on their mental health and development. The article also underscores the need for deepened awareness among parents, educators, and, mainly, children regarding the risks of unsupervised social media interactions. It examines various legal provisions, policies and guidelines in the Indian Legal System regarding protection of child protection, highlighting worldclass standards and efforts taken by the government and corporate companies to address the issues. The article culminates by offering practical recommendations for improving child safety measures against social media, enhancing media literacy and promoting collaborations between social media platforms, parents, and educators to create a safer and supportive mode of digital environment for children.

Social media, Cyberbullying, Cyber-security, Child Protection, Cyber-realism

Introduction

Social media has become an integral part of the internet. It has become the verbal platform where every human tries to explore things, creation, sharing and aggregation of content, which includes ideas, interests or any other form of emotion or expression. Under this comes social networking site which is a platform where people use to build social network and social relationships with other people who share similar content, idea of career. The number of social media users is increasing rapidly all over the world and it's no different in India. It has become an important part in the country's digital landscape, influencing everyone's personal space to professional life. The country's digital landscape is rapidly changing and with every shift, the social media also changes. Indians increasingly use this media for sharing experiences, building personal stuffs, and learning from the content shared by others. Over the years, social media interactions in India have soared, with more users joining daily to connect, express themselves, and participate in global interactions through their online interactions.

With over half of the online population of India and the total internet users on the rise, social media has become a place for connecting with friends, family and relative who live away from us. This not only ends with personal relationships but also extends to business contacts. People engage in business contacts and reach their

alien clients and customers through social media. Social media in India has become a hub for diverse ideas, enhancing previously ignored ideas and voices.

The 3 most used social media platforms in India as of 2024 are, Instagram (516.92 million active users), Facebook (492.70 million active users), X (Twitter) (296.87 million active users).¹

Table 1: Table And Obtained From Global Statistics

| Most Used Social Media Platforms In India | Percentage | Active Users(In Millions) |
|---|------------|---------------------------|
| Instagram | 74.70% | 516.92 |
| Facebook | 71.20% | 492.70 |
| X(Twitter) | 42.90% | 296.87 |

Social media users are not only adults but also children and teenagers. They are aged between 9 to 18. Children, in particular are increasingly addicted to social media platforms, spending considerable amount engaging in the content, interacting with people and in extreme cases, they engage in social media platforms that are meant for older users.

While discussing internet, we can't eliminate the benefits of it. Social media can provide benefits for some youth by providing positive community and connection with others who share same identities, abilities and interests. It can provide access to important information and create a space for self-expression.²

Internet provides with the following benefits:

- Near limitless information resource
- High degree of availability and affordability in most communities in the western world
- An asset for research on homework
- A communication tool for teachers and university professors with their students
- Rapid and inexpensive communication via e-mail and video linkage
- Access by the disabled to much that may otherwise be unavailable:
 - Through technology that makes computer use possible
 - By taking advantage of communication with peers that does not require that their disability be visible
- Source of entertainment

Research Problem

There is no explicit law that allows for the forceful prosecution of child cyberbullying. The Indian Constitution's protections for free expression also make it easy for social networking sites, internet service providers, and wrongdoers to evade responsibility. There is a gap in implementation and spread of knowledge of cyberbullying laws and rules.

Literature Review

According to a 2023 survey by Indian Council of Medical Research (ICMR)³, nearly 69% of children aged between 9 to 17 are active users of social media platforms. It also revealed that nearly 30% of the children a considerable time of 4 hours in social media platforms. This may lead to concerns on their mental health and social circle.

Additionally, a report by Klynveld Peat Marwick Goerdeler (KPMG) highlighted that nearly 58% of children face issues and risk of cyberbullying and 40% of parents rose concerns about their children being exposed to inappropriate content in social media.

The above statistics and reports rise the urgent need to address the risks proposed in the usage of social media and emphasise the need for improved legal framework in the country to govern the activity of social media and to educate children, parents and educators on social media usage and digital literacy.

Children face various risks in social media, from cyberbullying to privacy violation. With the growing dependence on social media and networking, platforms collect the platforms collect a plenty of personal data,

¹ Statistics obtained from Global Statistics

² Uhls, Y.T., Ellison, N.B., and Subramanyam, K. (2017). Benefits and Costs of Social Media in Adolescence. *Pediatrics*, 140(Suppl 2), S67-S70.

³ <https://pmc.ncbi.nlm.nih.gov/articles/PMC9407706/>

including the information that can be exploited by cyber criminals. Cyberbullying is an offence which includes threats, harassment and intimidation through social media platforms. Cyberbullying, being harmful in nature, is very destructive when it is done to children. It can deeply hurt the children's emotion and mental well-being. It is medically proven that prolonged exposure to cyberbullying can lead to anxiety and depression and can lead to suicidal thoughts in extreme situations.

Cyber bullying- definition

The word cyber bullying was first used by Bill Besley, a Canadian Educator. It is a form of bullying and harassment using information and communication technology to harm a person's reputation, mental mindset or to simply humiliate a person.

UNICEF defines Cyber Bullying as "it is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include:

- Spreading lies about or posting embarrassing photos or videos of someone on social media.
- Sending hurtful, threatening or abusive messages, images or videos via messaging platforms.
- Impersonating someone and sending mean messages to others on their behalf or through fake accounts.⁴

Though Cyber bullying is not explicitly defined in the Indian law, in the context of **IPC, 1860**⁵, cyber bullying refers to the use of online platforms or digital technologies to harass, threaten, or defame an individual. It also involves stalking, defamation, intimidation or harassment of the vulnerable through the digital media.

Impact of Cyber Bullying

When bullying happens online it can feel as if you're being attacked everywhere, even inside your own home. It can seem like there's no escape. The effects can last a long time and affect a person in many ways:

- **Mentally** – feeling upset, embarrassed, stupid, even afraid or angry
- **Emotionally** – feeling ashamed or losing interest in the things you love
- **Physically** – tired (loss of sleep), or experiencing symptoms like stomach aches and headaches

The feeling of being laughed at or harassed by others, can prevent people from speaking up or trying to deal with the problem. In extreme cases, cyberbullying can even lead to people taking their own lives. Cyberbullying can affect us in many ways. But these can be overcome and people can regain their confidence and health.⁶

Addition to cyberbullying, children are exposed to inappropriate and explicit content through social media such as explicit sexual content, violent content and grooming behavior. These can affect the psychological development of the children. For instance, some time back, 'the Blue Whale Challenge' rose into prominence. It was a viral social media game that involved a series of dangerous tasks, finally reaching to encourage suicidal thoughts to the participants. It targeted vulnerable teenagers who were addicted to social media. It resulted in many children aged between 9 to 18 committing suicides as a result of the game. The peer pressure developed from social media compels many children to engage in certain behaviors. Most important is the addictive nature of social media leads to children using it most of the time and thus leading to dip in academic performance and social skills.

International Legal Framework on Social Media crimes and Cyberbullying to children:

1. United States of America

The states of California, Connecticut, Colorado, and Illinois have implemented cyberbullying laws by punishment including suspension and expulsion. The federal law of Megan Meier Cyber bullying Prevention Act, 2009 imposes penalty on anyone who communicates with another with intention to coerce, harass, intimidate or cause substantial emotional distress through electronic means.⁷ Children's Online Privacy Protection Act (COPPA), 1998⁸ protects children online and from cyberbullying.

⁴ Unicef.org – Cyberbullying: what is it and how to stop it?

⁵ Indian Penal Code, 1860

⁶ Unicef.org – Cyberbullying: what is it and how to stop it?

⁷ H.R.1966 - Megan Meier Cyberbullying Prevention Act 1966, Acts of Parliament, 1966 (US)

⁸ Children's Online Privacy Protection Act (COPPA), 1998 <https://www.ftc.gov> (United States of America)

2. United Kingdom

The UK has several laws to protect children from cyberbullying. They are:

- *Protection from Harassment Act 1997*⁹: this act prohibits harassment and other similar conducts that affect children and adolescents.
- *Malicious Communications Act 1988*¹⁰: this act makes it illegal to send indecent, offensive, or threatening electronic communications.

3. International View on Cyberbullying

UNICEF, in coordination with the **United Nations**, ask the countries all over the world to make laws that specify cyberbullying against children, as they see children's protection from online and digital media is the need of the hour. Many countries have recognised cyberbullying as a serious crime and have made laws to prevent and prohibit cyber bullying, specifically against children.¹¹

Legal Framework In India Regarding Child Safety And Exploitation From/ By Social Media

1. Constitutional Provisions Related to Social Media and Children's Rights

Article 19 (1)(a) of the Indian Constitution guarantees the right to freedom of speech and expression, which encompasses the use of social media for sharing thoughts and ideologies. On the other hand, Article 19(2) imposes certain restrictions such as decency, morality and public order. This can be invoked to regulate harmful and inappropriate content in social media which includes those which affects child's safety.

Article 21 of the Indian Constitution, which deals with right to life and personal liberty, recognized 'right to privacy' as a fundamental right, as interpreted in the landmark Puttaswamy judgment. This has reaching implication on social media regulations, where children's safety is often compromised. This iconic recognition has put additional pressure on digital media platforms to protect personal privacy of children.

2. Provisions in the IPC

The press release of 'Digital Exploitation of Children', in 2019, by the Ministry of Women and Child Development states that **Sections 354A and 354D**¹² provides punishment for cyberbullying and cyber stalking against women and children.¹³

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

The Juvenile Justice (Care and Protection of Children) Act, 2015 mandates the protection of children from exploitation, which includes online exploitation. Section 2(14)¹⁴ of this act defines who is a child. It says that anyone below 18 years of age is a child and establishes a legal framework for all protective measures for minors.

4. Information Technology (IT) Act, 2000

India's Information Technology (IT) act, 2000 stays a cornerstone in the Indian legal system to govern and regulate cyber activities. It aims to provide a framework for e-commerce and the prevention of cybercrime. It includes special provisions to protect children and teenagers. Notably, Section 66E¹⁵ of the act addresses the privacy violation and outlines that capturing, publishing and transmitting the private area of a person without the consent of the person involved. This section protects the children's privacy in social media indirectly. Section 67B of this act specifically targets child pornography and prohibits the publishing and transmitting of any material depicting children involved in sexual acts. This provision aims to curb the circulation of harmful content targeting minor children.

Cyber stalking includes, *inter alia*, the following:

- Sending threatening or obscene messages, posts or emails;
- Stealing a person's identity online and circulating false information with the intent to humiliate or harass;
- Tracing the location of a person through illegal means;

⁹ Protection from Harassment Act, 1997(United Kingdom)

¹⁰ Malicious Communications Act, 1988(United Kingdom)

¹¹ *International Perspectives on Cyberbullying* by Baldry, A., Blaya, C. and Farrington, D.

¹² Section 354D and 354A of Indian Penal Code, 1860

¹³ Pib.gov.in *Digital Exploitation on Children*

¹⁴ Section 2(14) of Juvenile Justice (Care and Protection) Act, 2015 Bill No 99-C of 2014

¹⁵ Section 66E of Information Technology Act, 2000

- Uploading obscene pictures;
- Posting derogatory remarks online with the intent to harass.

5. POCSO Act, 2012

The POCSO Act is designed to address the sexual exploitation of children, including online grooming and the dissemination of child sexual abuse material (CSAM). Section 3¹⁶ defines various forms of sexual assault against children, including those perpetrated through digital means. Section 5 addresses aggravated sexual assault, including situations where the offender uses a digital platform to exploit a child.

6. Personal Data Protection Bill, 2019¹⁷

This bill is a promising bill prepared by the Indian Legal System to safeguard online privacy. This bill includes specific provisions to protect children's data from online and digital dangers. Chapter 6 (Section 6) demands digital platforms to obtain consent before processing minor's personal data, supporting the importance of safeguarding children's safety and privacy. Section 23 mandates that data fiduciaries (organizations that handle data) take additional care when processing children's data, acknowledging their vulnerability.

Common legal provisions include the following:

| Offence | Legal Provision |
|--------------------------------|----------------------------------|
| 1. Cyber Bullying | IPC Sec. 503, 506 and 507 |
| 2. Cyber stalking | IPC Sec. 354D, 509 |
| 3. Identity theft | POCSO Sec. 11(iv) |
| 4. Violation of Privacy | ITA Sec. 66A |
| 5. Hacking | ITA Sec. 66E, 72 |
| 6. Child Sexual Abuse Material | POCSO Sec. 23 |
| 7. Sexual Harassment | ITA Sec. 43, 66 |
| | POCSO Sec 11 (v) & (vi), 13 – 15 |
| | ITA Sec. 66E, 67 |
| | IPC Sec. 292, 354A(1)(iii), 354C |
| | POCSO Sec. 11 |
| | IPC Sec. 354A, 509B |

In the 2014 case of **Kamlesh Vaswani v. Union of India**¹⁸, Kamlesh filed a public Interest Litigation (PIL) seeking a ban on websites that hosted pornographic content, stating that such content contributed to sexual violence against children. The Supreme Court carefully reviewed the petition and was worried about children having easy access to inappropriate content. While the case didn't lead to a total ban on pornographic websites, it led to actions to reduce access to harmful material, especially for minors.

Later, in 2015, in the **Shreya Singhal v. Union of India case**¹⁹, they challenged the constitutionality of Section 66A of the Information Technology (IT) Act, 2000, which allowed for the arrest of individuals posting offensive content in digital media. The case indirectly focused to prevent children to be exposed to offensive content in social media. The Supreme Court struck down Section 66A for being vague and overly broad, violating the right to freedom of speech and expression under Article 19(1)(a). However, it highlighted the need for clear legal frameworks for regulating online content.

In the **K.S. Puttuswamy v. Union of India (2017) case**²⁰, The Supreme Court declared the right to privacy a fundamental right under Article 21 of the Constitution, which has significant implications for children's online privacy, particularly regarding data collection by social media platforms. The judgement emphasised the protection of personal data, which is crucial in safeguarding children's privacy in digital media. This case laid

¹⁶ Section 3 of The Protection of Children from Sexual Offences Act, 2012

¹⁷ Personal Data Protection Bill, 2019

¹⁸ Kamlesh Vaswani v Union of India (2014) 6 SCC 705

¹⁹ Shreya Singhal v. Union of India (2013) 12 SCC 73

²⁰ K.S. Puttuswamy v. Union of India (2017) 10 SCC 1

to foundation for the proposed Personal Data Protection Bill, 2019 and raised awareness about the need to protect minors from data exploitation by tech companies and social media platforms.

In Re: Prajwala Letter dated 18.2.2015 Videos of Sexual Violence and Recommendations, Child Sexual Abuse Material (CSAM) Online case was initiated after an NGO brought to the Supreme Court's attention videos depicting sexual violence that included child sexual abuse, circulating on social media platforms and messaging services. The Supreme Court directed the government to take proactive steps to curb the dissemination of such content online. It led to orders requiring social media companies to introduce mechanisms for content takedown and reporting, highlighting the role of platforms in preventing the spread of child sexual abuse material.

Challenges Faced In Enforcement Of Child Protection Laws

1. Awareness on Digital Literacy- A critical challenge in the enforcement of laws surrounding children's safety on social media is the lack of awareness and digital literacy among key stakeholders, such as parents, children, educators, and even law enforcement agencies. Many parents and teachers, who play a vital role in guiding children in their online activities, are often unaware of the existing legal frameworks designed to safeguard their children. This unawareness leaves children vulnerable to the dangers of the digital world, as they are not educated on the potential risks associated with social media and internet use. Furthermore, law enforcement agencies, who are responsible for investigating and prosecuting online offenses, often lack the specialized knowledge required to navigate the complex digital landscape. Without proper training and tools, they struggle to educate children on safe internet practices or to enforce the laws effectively. This gap in digital literacy and awareness hinders the ability to protect children from online harm.

2. Jurisdiction Issues- One of the most significant challenges in enforcing laws related to children's safety on social media is the issue of jurisdiction. Social media platforms operate globally, often headquartered in countries outside India, and cybercrimes can be committed from anywhere in the world. When an offense occurs on a platform or website based in a foreign country, Indian law enforcement agencies often find themselves unable to prosecute the offenders due to jurisdictional limitations. International actors who commit offenses, such as online harassment, exploitation, or abuse against Indian children, can escape justice if they are located in a country with different legal frameworks. These cross-border complexities make it difficult for Indian law to effectively bring such offenders to justice, thus posing a significant barrier to the protection of children on digital platforms.

3. Enforcement and Policy Making- India's legal and law enforcement systems face serious challenges when it comes to tackling cybercrimes involving children. These crimes, which often require a deep understanding of digital technologies, are frequently beyond the scope of traditional training that law enforcement agencies receive. Investigators and prosecutors are often under-equipped and under-trained to handle such cases, leading to delays in investigations and a backlog in prosecutions. This slow response leaves victims, often children, unprotected and vulnerable to further harm. Moreover, the rapid evolution of technology and digital platforms outpaces the development of laws and policies, meaning that the legal frameworks governing online safety are often outdated or insufficient to address the sophisticated methods used by cybercriminals. Strengthening the capacity of law enforcement, updating policies, and ensuring faster, more efficient responses to online threats is crucial for protecting children in the digital age.

Government Measures

The **Ministry of Electronics and Information Technology (MeitY)**²¹ has taken several steps to promote cyber hygiene and protect users from digital threats. One notable initiative is the **Cyber Swachhta Kendra**²², which assists users in cleaning their systems from malware and promotes safe online behaviour by raising awareness about cybersecurity practices. Additionally, **MeitY**²³ runs awareness campaigns targeting individuals and organizations, highlighting the importance of securing personal information online. However, despite these efforts, there is a significant gap when it comes to initiatives specifically aimed at safeguarding children from the unique threats they face online. The growing presence of children on social media and digital platforms necessitates tailored programs focused on their protection, which are currently lacking.

²¹ Ministry of Electronics and Information Technology <https://www.meity.gov.in>

²² <https://www.csk.gov.in>

²³ Supra note 21

Corporate Responsibility

Many social media companies, such as Meta (Facebook, Instagram) and Google (YouTube), have introduced tools to help parents and guardians monitor their children's online activities. These include parental controls, restricted modes, and systems that allow users to report inappropriate or harmful content. While these features are useful, they often fall short in preventing the circulation of harmful content. The systems in place to manage content moderation and accountability are not robust enough, leading to incidents of cyberbullying, online exploitation, and exposure to inappropriate material that continue to affect children across digital platforms. Strengthening these tools and increasing corporate responsibility remain crucial challenges.

Need for Specific Legal Provisions on Cyberbullying

The digital landscape is evolving rapidly, and while social media offers unprecedented opportunities for connectivity, creativity, and self-expression, it also exposes children to significant risks. Children are increasingly vulnerable to cyberbullying, online predators, exposure to inappropriate content, and data privacy violations. In India, existing legal frameworks like the Information Technology Act (2000)²⁴ and amendments have made strides toward protecting minors online, but critical gaps in enforcement and awareness persist. These gaps, if not addressed, leave children exposed to online dangers, despite the availability of legal safeguards.

A key issue is the lack of awareness among parents, educators, and even children themselves about the risks they face online. Comprehensive public awareness campaigns aimed at parents, children, and educators can empower users to navigate the digital landscape responsibly. Schools and community centres should also play a pivotal role in digital literacy education, teaching children not just about internet safety but about ethical online behaviour.

Moreover, the need for increased cooperation between government bodies, social media platforms, and educational institutions is critical. Government agencies can enforce stronger policies, while social media platforms can improve their content moderation and parental control tools. These collaborations will be essential to creating a safer digital environment for children.

The government may form a permanent committee that looks over the issues of children faced by the dark side of the social media. It can take regular statistics on the form of social media the children use, using the Media History Form developed by the Canadian Paediatric Society (CPS) and the Media Awareness Network.²⁵

A Report of Ad-Hoc Committee of the Rajya Sabha on the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a Whole²⁶, presented in January 2020, has recommended an amendment in Section 11 clause (iv) of the POCSO Act²⁷ to add a new provision “cyber grooming” to tackle the problem of grooming.

The National Commission for Protection of Child Rights (NCPCR)²⁸ is a statutory body established under Section 13 the Commission for Protection Of Child Rights Act, 2005²⁹. This act aims at protecting children's rights. When the government gives independence and autonomous powers, the commission can significantly enhance its ability to address children's issues. It could effectively enforce child protection laws and amend them, focusing on cyber bullying and social media threats, collaborate with other relevant legal bodies and respond swiftly to the issues. This may ensure child safety in the digital space.

In conclusion, to truly safeguard children in the digital age, it is imperative to enact and enforce robust laws that specifically target online exploitation, harassment, and abuse. Only through a collective, multi-faceted approach can we ensure that children benefit from social media's advantages without being endangered by its darker side.

²⁴ Information Technology Act, 2000 (Supra note 14)

²⁵ Media Awareness Network and Canadian Paediatric Society . Media History Form in Media Pulse: Measuring the Media in Kids' Lives, A Guide for Health Professionals. Ottawa: Canadian Paediatric Society and Media Awareness Network; 2003

²⁶ Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a Whole, Jan. 25, 2020, Rajya Sabha, Parliament of India, https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf

²⁷ Supra Note 15

²⁸ <https://ncpcr.gov.in>

²⁹ Section 13 of Commission for Protection of Child Rights Act, 2005