IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Protecting Our Children From Cybercrime On Social Media Platforms

GARIMA SINGH
PhD Research Scholar
FACULTY OF LAW
S.S.J. University (Almora)

Abstract: In the digital age of today, children make up a huge and basic segment of the population on the web. Children are spending even more time on the Internet. As a result of excessive use of computers and the internet children are becoming more vulnerable to cybercrime including bullying, data theft, fraud, harassment and other harmful behaviour and content. Cases of online sexual abuse and exploitation of children have surged in India and worldwide. Although the government is taking all the possible efforts to tackle the menace of cybercrime against children, yet a lot has to be done. The present study aimed at exploring the problem of cybercrime against children in India. This is a comparative study based on doctrinal method dealing with data collected from primary as well as secondary resources. This research is descriptive and analytical in nature. The objective of this study is to explore, examine and analyze the legal provisions regarding cybercrime against children.

Keywords- Children, Cyber Crime, Cyber Security, Online Offence

Introduction

In the digital age, social media has revolutionized the way people connect, communicate, and consume information. children make up a huge and basic segment of the population on the web. While these platforms offer numerous benefits, they have also become fertile ground for various forms of cybercrime. As a result of excessive use of computers and the internet children are becoming more vulnerable to cybercrime including bullying, data theft, fraud, harassment and other harmful behaviour and content. Cases of online sexual abuse and exploitation of children have surged in India and worldwide. Although the government is taking all the possible efforts to tackle the menace of cybercrime against children, yet a lot has to be done.

According to a report by UNICEF, over **175,000 children go online for the first time every day**, and the number continues to rise as smartphones and affordable internet access reach every corner of the world.[1] In India, where more than **400 million internet users** are under the age of 18, the situation demands urgent attention.[2] The prevalence of cyber bullying, online grooming, sextortion, and exposure to harmful content through social media platforms such as Instagram, Facebook, and TikTok has sparked grave concern among parents, educators, and policymakers.

While there are legislative safeguards in place, such as the **Information Technology Act, 2000**, and the **Protection of Children from Sexual Offences (POCSO) Act, 2012**, these frameworks are often found wanting when confronting the dynamic, cross-border nature of cybercrime. Furthermore, many social media companies fail to provide adequate protections or timely interventions, leaving minors exposed to significant risks.

The aim of this research paper is to provide a comprehensive legal and social analysis of the challenges posed by cybercrime to children using social media in India. It will examine the types of cyber threats

[1] https://www.unicef.org/publications/index_101992.html,UNICEF. *Children in a Digital World*. 2017.

[2] https://www.thehindu.com, India has over 400 million internet users under 18: UNICEF." *The Hindu*, 12 Dec. 2019.

faced by children, the adequacy of existing legal and institutional frameworks, the role of social media platforms, and strategies for prevention and protection. Emphasis will also be placed on comparative perspectives, case studies, and recommendations for effective and holistic interventions.

2. Understanding Cybercrime and Social Media

Social media platforms such as Facebook, Instagram, WhatsApp, Snapchat, and TikTok have emerged as essential tools of communication and socialization for children and teenagers. However, these platforms are also fertile ground for cybercriminals, who exploit the anonymity and vast user base of social media to target vulnerable users especially minors. Understanding the landscape of cybercrime and how it intersects with social media is key to developing appropriate protective mechanisms.

2.1 What is Cybercrime?

Cybercrime refers to any criminal activity that involves a computer, networked device, or a network. When such crimes are directed at or affect children, the consequences can be particularly damaging. These crimes can range from relatively low-level harassment and bullying to more serious offenses such as child pornography, grooming, and trafficking. According to the Indian Ministry of Home Affairs, cybercrime against children in India has grown by over 400% in the past five years, with a significant number of incidents linked to social media platforms.[3]

Cybercrime, when discussed in the context of children and social media, includes a wide spectrum of offenses:

- **Cyberbullying**: Deliberate and repeated harm inflicted through electronic devices. According to UNICEF, Cyberbullying 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.[4]
- **Online Grooming**: when someone uses the internet to build a relationship with a minor person, with the intention of tricking, pressuring or forcing them into doing something sexual, like sending images or videos of themselves.[5]
- **Sextortion**: Sextortion is a form of child sexual exploitation where children are threatened or blackmailed, most often with the possibility of sharing with the public a nude or sexual images of them, by a person who demands additional sexual content, sexual activity or money from the child. This crime may happen when a child has shared an image with someone they thought they knew or trusted, but in many cases they are targeted by an individual they met online who obtained a sexual image from the child through deceit, coercion, or some other method.[6]
- **Identity Theft**: Misuse of personal data such as names, photos, and school details.
- **Exposure to Inappropriate Content**: Inappropriate content includes information, images or material that's directed at adults. This might also include inaccurate information or information that might lead or tempt child into unlawful or dangerous behaviour.[7] It can take many shapes, and impacts on wellbeing depend on each child. It ncluding hate speech, pornography, and extremist propaganda.

These offenses often overlap and escalate quickly from emotional distress to psychological trauma, and in some tragic cases, even suicide.

2.2 Features of Social Media That Enable Cybercrime

Social media platforms, by design, promote connection, self-expression, and openness. While these features can be empowering, they also expose children to several risks:

- **Anonymity and Fake Profiles**: The ease of creating fake identities makes it difficult to identify perpetrators of cybercrime.
- **Private Messaging and Vanishing Chats**: Many apps support private conversations and disappearing messages, making detection and reporting harder.
- **User-Generated Content and Algorithms**: Platforms often push content based on user behavior, which can inadvertently expose children to inappropriate or harmful material.

---

[3] Ministry of Home Affairs, Government of India, *Cyber Crime in India: Annual Report*, 2023.

[4] https://www.unicef.org/end-violence/how-to-stop-cyberbullying, Cyberbullying: What is it and how to stop it

[5] https://www.ceopeducation.co.uk/11_18/lets-talk-about/sexual-abuse/online-grooming/

[6] https://www.missingkids.org/theissues/sextortion

[7] https://www.internetmatters.org

For example, TikTok, which is immensely popular among children, has been criticized for enabling predators to contact minors directly, despite its age restrictions.[8]

2.3 Real-World Impact

India has witnessed a disturbing rise in cybercrimes targeting minors. In 2022, a 15-year-old girl from Uttar Pradesh took her own life after repeated online harassment by a stalker who used morphed images of her on Instagram. The perpetrator used a fake profile and managed to evade detection for several months.[9] Similarly, in a 2021 case in Bengaluru, a 14-year-old boy was groomed through an online gaming platform and coerced into sending inappropriate pictures, which were then used for blackmail. The child was too scared to inform his parents, and the incident only came to light when school authorities noticed behavioral changes.[10]

2.4 Data on Children and Cybercrime in India

The **National Crime Records Bureau (NCRB)** recorded over **1,200 cases** of cybercrime against children in 2022 alone, but experts believe the actual number is much higher due to underreporting.[11] A majority of these incidents occurred on platforms like WhatsApp and Facebook, where regulatory oversight is minimal, and children can easily bypass age restrictions.

The prevalence of smartphones and low-cost internet has meant that children are going online unsupervised at increasingly younger ages. As per a 2023 report by Internet and Mobile Association of India (IAMAI), nearly **60% of internet users aged 12–17** access social media daily.[12] A national survey conducted in India found that Six out of 10 youngsters in the 9-17 age group spend over three hours daily on various social media sites.[13] Without adequate awareness and digital literacy, these children become easy targets for predators.

3. Vulnerabilities of Children in the Digital Space

While the internet provides unparalleled access to education, entertainment, and social interaction, it also presents a complex web of threats—especially for children. The digital space is inherently risky due to the anonymity it allows and the lack of real-time monitoring. Children, with their cognitive and emotional immaturity, are particularly susceptible to manipulation, deception, and exploitation on social media platforms. This section explores the multifaceted vulnerabilities of minors in cyberspace and how these are weaponized by cybercriminals.

3.1 Psychological and Developmental Vulnerabilities

Children and adolescents are in a critical stage of psychological development. Their prefrontal cortex—the part of the brain responsible for decision-making, impulse control, and assessing risk—is not fully developed until their mid-20s.[14] This makes them more likely to:

- Trust strangers online.
- Share personal information without understanding the consequences.
- Engage in risky behavior like sexting or oversharing.
- Be influenced by peer pressure or social validation through likes and shares.

Cybercriminals exploit these traits to manipulate minors into doing things they would not ordinarily do, such as sharing explicit content or meeting in person.

Moreover, children are often driven by a need for social acceptance, which makes them susceptible to online dares, trends, or "challenges" that can have dangerous outcomes. The viral "Blue Whale Challenge," which encouraged self-harm, is one such horrifying example that resulted in multiple teen

---

[8] https://thewire.in,Sahu, Priya. "TikTok Under Fire: The Dangers Children Face on Social Media." *The Wire*, 14 Mar. 2022.

[9] https://www.indiatoday.in,"Teen Girl Dies by Suicide After Cyberstalking Incident." *India Today*, 25 Nov. 2022.

[10] https://timesofindia.indiatimes.com,"Cyber Grooming on the Rise in Bengaluru Schools." *The Times of India*, 18 May 2021.

[11] National Crime Records Bureau (NCRB). *Crime in India 2022*. Ministry of Home Affairs, 2023.

[12] Internet and Mobile Association of India. *Digital in India Report 2023*, IAMAI, 2023.

[13] https://timesofindia.indiatimes.com/city/mumbai/60-children-spend-3-hours-a-day-on-social-media-study/articleshow/103878956.cms

[14] Steinberg, Laurence. *Age of Opportunity: Lessons from the New Science of Adolescence*. Houghton Mifflin Harcourt, 2014.

suicides globally, including in India.[15] According to US surgeon general Dr Vivek Murthy's report 2022 said , social media interactions increases the risk of mental health problems such as depression and anxiety among children.[16]

Social media interactions increases the risk of mental health problems such as depression and anxiety among children.

3.2 Online Grooming and Predatory Behavior

Online grooming is a deliberate and methodical process used by sexual predators to gain a child's trust before engaging in sexual abuse or exploitation. Groomers often pose as peers or mentors and gradually build a relationship through compliments, attention, and gifts before introducing inappropriate content or requests.

The POCSO Act defines and criminalizes such conduct, yet grooming often goes unreported due to fear, shame, or lack of awareness.[17] With features like private chats, encrypted messaging, and disappearing content, it has become increasingly easy for predators to avoid detection.

In a 2020 case from Maharashtra, a 13-year-old girl was groomed by a 40-year-old man posing as a school student on Instagram. He used flattery and shared memes to gain her confidence before requesting inappropriate pictures and threatening her with exposure.[18]

3.3 Cyberbullying and Social Harassment

Cyberbullying refers to the use of digital communication tools to harass, threaten, or humiliate someone, and it is especially rampant among teenagers. Common forms include:

- Spreading rumors or defamatory content.
- Creating fake profiles.
- Sending threatening messages.
- Public shaming via photos or videos.

A 2022 survey by the National Commission for Protection of Child Rights (NCPCR) found that **over 37% of Indian children aged 13–17** reported experiencing cyberbullying, mostly on WhatsApp and Instagram.[19] Victims often suffer from anxiety, depression, and social withdrawal. In extreme cases, it has led to suicide.

What makes cyberbullying particularly harmful is its 24/7 nature—it can follow children into their homes, giving them no safe space to escape.

3.4 Sextortion and Image-Based Abuse

Sextortion refers to the threat of sharing sexual images or videos of a person unless they meet certain demands, which are often sexual in nature. Children may be coerced into sending explicit photos, which are then used as blackmail material.

Even consensual sharing of images—commonly known as "sexting"—can lead to unintentional harm. If those images fall into the wrong hands, they can be distributed widely across social media and pornographic websites, causing irreversible psychological trauma.

In 2021, a Delhi-based 16-year-old boy committed suicide after falling victim to sextortion. He had shared a private video with someone he thought was a girl, who later demanded money and threatened to leak it. The shame and fear drove him to take his own life.[20]

3.5 Misinformation, Radicalization, and Unsafe Content

Children are frequently exposed to harmful and misleading content on social media:

- **Fake news** can manipulate their understanding of events and politics.

---

[15] https://www.ndtv.com,"Blue Whale Challenge: How Online Games Can Be Fatal for Teens." *NDTV*, 27 Aug. 2017.

[16] http://timesofindia.indiatimes.com/articleshow/103878956.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[17] Protection of Children from Sexual Offences (POCSO) Act, 2012. Government of India.

[18] https://www.hindustantimes.com,"Maharashtra Girl Groomed Online: Instagram Used to Lure Minor." *Hindustan Times*, 9 July 2020.

[19] National Commission for Protection of Child Rights. *Cyber Safety of Children Survey Report*, 2022.

[20] https://www.thehindu.com,"Teen Suicide in Delhi Linked to Sextortion." *The Hindu*, 22 Mar. 2021.

- **Hate speech** can normalize discrimination and violence.
- **Radical content** can lead to self-harm, substance abuse, or even criminal behavior.

Social media algorithms prioritize content that is sensational and emotionally charged, making it more likely for children to encounter dangerous material. Despite content moderation policies, the sheer volume of uploads makes it impossible to filter everything in real-time.

In 2023, YouTube came under fire after reports revealed that its algorithm had recommended violent extremist content to underage users despite their account settings being in "restricted mode.[21]

4. Legal Framework Protecting Children

Children's vulnerability in cyberspace has triggered global and national efforts to build robust legal frameworks aimed at their protection. In India, several laws address various dimensions of cybercrime, especially where children are concerned. However, legal enforcement faces challenges due to technological evolution, cross-border jurisdiction issues, and the anonymity of online platforms. This section analyzes both **international and Indian legal instruments**, highlighting their strengths and shortcomings.

4.1 International Legal Instruments

International bodies such as the United Nations (UN) and the International Telecommunication Union (ITU) have taken significant steps toward the protection of children in the digital age.

4.1.1 United Nations Convention on the Rights of the Child (UNCRC)

The **UNCRC**, ratified by India in 1992, lays the groundwork for the protection of children's rights in all spheres, including the digital one. Articles 16 and 17 emphasize a child's right to privacy and access to appropriate information.[22] While the Convention predates widespread internet usage, its principles are relevant to online safety.

In 2021, the UN Committee on the Rights of the Child adopted **General Comment No. 25**, which specifically addresses children's rights in the digital environment, urging states to ensure protection against digital risks while promoting access to beneficial online content.[23]

4.1.2 ITU's Child Online Protection (COP) Guidelines

The **ITU's COP Guidelines**, updated in 2020, are a comprehensive set of recommendations for governments, industry, parents, and educators. They stress the importance of age-appropriate content, platform accountability, and international cooperation.[24]

4.2 Indian Legal Framework

India has developed a multi-layered legal architecture to protect children against online crimes. This includes both general cyber laws and child-specific protections.

4.2.1 The Information Technology Act, 2000 (IT Act)

The IT Act is the primary legislation governing cyber activities in India. Several provisions are applicable to crimes involving minors:

- **Section 66E**: Punishes the violation of privacy by capturing, publishing, or transmitting images of private areas without consent.
- **Section 67 and 67B**: Address the publication or transmission of obscene material and explicitly prohibit child pornography and exploitative content involving minors.
- **Section 69A**: Grants the government authority to block websites or platforms that host harmful or illegal content.

However, these sections often fall short when it comes to swift enforcement, especially when dealing with foreign-based platforms like Facebook or Instagram that operate under different legal jurisdictions.[25]

---

[21] https://www.theguardian.com,Paul, Kari. "YouTube Recommended Violent Content to Children, Says Report." *The Guardian*, 6 Sep. 2023.

[22]www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child, United Nations Convention on the Rights of the Child, 1989.

[23] UN Committee on the Rights of the Child. *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, 2 Mar. 2021.

[24]www.itu.int/en/cop,International Telecommunication Union, *Child Online Protection Guidelines 2020*.

[25]https://www.barandbench.com, Basu, Saptarshi. "IT Act and Its Application in the Age of Global Social Media Giants," *Bar and Bench*, 19 May 2023.

4.2.2 Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO Act criminalizes a wide range of sexual offenses against children and includes provisions for digital evidence and online exploitation:

- **Section 11 and 12**: Define and penalize sexual harassment, including online gestures or messages of a sexual nature.
- **Section 13–15**: Specifically address the use of children in pornography, including online transmission and storage of such content.
- **Section 27**: Ensures the confidentiality of the child victim's identity and protection during trial.

POCSO has become crucial in prosecuting cyber grooming and sextortion cases. Still, challenges like lack of digital literacy among law enforcement and procedural delays hinder timely justice.

4.2.3 **Bharatiya Nyaya Sanhita(BNS),2023**

which came into effect on July 1, 2024, replaces the Indian Penal Code (IPC)

Sections of the BNS are also invoked in cybercrime cases against children, including:

Section 78 (1) Any man who— (i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or (ii) monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking: Provided that such conduct shall not amount to stalking if the man who pursued it proves that— (i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or (ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or (iii) in the particular circumstances such conduct was reasonable and justified. (2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

Section 79- Whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object in any form, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine.

Section 351-357- Criminal intimidation, which includes threats made via digital platforms.

Though not originally designed for cyber-related offenses, these provisions are frequently adapted to fit digital crimes.

4.3 Recent Legislative and Regulatory Developments

India has been making strides toward digital regulation to protect users—especially children.

4.3.1 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules impose stricter accountability on social media intermediaries:

- Require platforms to **remove offensive content within 24–72 hours** of complaint.
- Mandate the **appointment of grievance officers**.
- Enforce **age verification mechanisms** for content hosting services.

While the intent is commendable, implementation has been uneven. Critics argue that tech companies often delay compliance or interpret the rules loosely.[26]

4.3.2 Data Protection Laws (Proposed Digital Personal Data Protection Act, 2023)

The **Digital Personal Data Protection Act**, passed in 2023, provides explicit provisions for processing children's data:

- Defines a "child" as an individual under 18 years of age.
- Requires verifiable **parental consent** for data collection and processing.
- Prohibits tracking, behavioral advertising, or targeted messaging to children.

These provisions echo similar laws like the **Children's Online Privacy Protection Act (COPPA)** in the U.S., but critics fear poor enforcement due to lack of infrastructure and awareness.

4.4 Gaps and Challenges in the Legal Framework

Despite the presence of multiple laws, several gaps persist:

- **Jurisdictional Issues**: Offenders may operate from outside India, making enforcement difficult.

[26] https://economictimes.indiatimes.com,"India's New IT Rules and the Challenge of Platform Accountability." *The Economic Times*, 7 June 2023.

- **Delayed Investigation and Poor Forensics**: Many police stations lack technical capacity to trace digital crimes.
- **Platform Evasion**: Many social media platforms fail to verify users' ages or act quickly on abuse reports.
- **Underreporting**: Victims, especially children, often feel scared or ashamed to report incidents.

These gaps necessitate a more integrated and proactive approach involving legal reform, better policing, and public-private collaboration.

5. Role of Social Media Platforms

Social media platforms are central to the modern digital experience of children, acting both as spaces for creativity and interaction as well as arenas for significant risk. Given their influence, these platforms play a critical role in ensuring user safety, particularly for minors. This section explores the existing measures taken by major platforms, evaluates their effectiveness, and highlights the accountability they bear within the legal and ethical ecosystem.

5.1 Popular Platforms Used by Children in India

Children and teenagers in India frequently engage with the following platforms:

- **Instagram**: Known for photo and video sharing, popular among teenagers.
- **WhatsApp**: Widely used for private messaging and group chats.
- **YouTube**: The most used platform for video consumption and even content creation.
- **Facebook**: Though less popular with younger users now, still used for social networking.
- **Snapchat** and **Discord**: Gaining traction due to disappearing messages and interactive gaming chats.

According to a 2023 report by Internet and Mobile Association of India (IAMAI), **over 45% of internet users aged 10–18 years** in urban India actively use at least one of these platforms daily.[27]

5.2 Policies for Child Protection: An Overview

Most major platforms have articulated **community standards**, **content policies**, and **age restrictions** to ensure safety:

Instagram

- Minimum age requirement of **13 years**.
- "Private by default" for users under 16.
- **AI-based content filtering** and reporting features for offensive content.
- "Take a Break" and **parental supervision tools** introduced in 2022.

YouTube

- Offers **YouTube Kids**, a platform tailored to child-safe content.
- Restricts monetization and comments on videos uploaded by minors.
- **Automatic flagging system** for potentially harmful content.

WhatsApp

- Claims end-to-end encryption, but this also hampers monitoring.
- Introduced **report and block** features and **admin controls** for group chats.
- New **safety campaigns** in India targeting schoolchildren.

Despite these initiatives, platforms often fall short of timely intervention, and their AI moderation can miss context-sensitive threats, such as grooming, subtle bullying, or coded hate speech.

5.3 Self-Regulation vs. Legal Obligation

Social media companies typically follow a **self-regulatory** model based on internal guidelines and terms of service. However, self-regulation is **not legally enforceable**, and there's considerable variation in how effectively platforms implement their own rules.

Under India's **IT Rules, 2021**, social media intermediaries with more than 5 million users must:

- Appoint a **grievance redressal officer in India**.
- Publish monthly transparency reports.
- Remove content within 24 hours of a complaint involving child safety.

While companies like Meta (which owns Facebook, Instagram, and WhatsApp) have complied on paper, **ground-level response to user complaints remains slow**, and many safety issues go unresolved for weeks.

In 2023, the **Delhi High Court**, in *XYZ v. Meta Platforms Inc.*, criticized Meta for failing to act against a user who had impersonated and blackmailed a minor girl. The court called for "stringent liability" for platform negligence.[28]

[27] Internet and Mobile Association of India. Digital Adoption and Online Safety Report 2023.

5.4 Technical Safeguards and Limitations

AI and Machine Learning

Platforms increasingly rely on AI to flag inappropriate content. While this allows real-time moderation at scale, AI can:

- Misinterpret satire or coded language.
- Miss images/videos shared via encrypted or closed groups.
- Get bypassed by intentional misspellings and emojis.

Age Verification Mechanisms

Most platforms only use **self-declared age**, which is easy to falsify. Even though some are experimenting with AI age-estimation through facial recognition, **privacy concerns** and legal challenges limit widespread adoption.

Reporting and Blocking Tools

Available on all major platforms, these tools empower users to report abuse. However:

- **Underreporting** is rampant due to shame or fear.
- **Follow-up is inconsistent**—some reports are resolved quickly, others ignored.

In a 2022 study by the Centre for Internet and Society, 62% of children who faced abuse online reported that their complaints went **unacknowledged by platforms**.[29]

5.5 Industry Collaboration and Safety Campaigns

In India, tech giants have launched collaborative initiatives with NGOs and governments:

- **Meta's 'We Think Digital' Campaign**: Educates children about online etiquette, safety, and misinformation.
- **Google's 'Be Internet Awesome'**: A curriculum designed to teach kids digital safety in schools.
- **YouTube's Creator Academy**: Trains content creators to comply with child protection guidelines.

While these initiatives are laudable, **they often remain confined to urban schools** and are inaccessible to rural or underprivileged communities—where awareness is most needed.

5.6 Criticism and the Need for Greater Accountability

Social media companies are often accused of **putting profits before safety**. Algorithms that promote engagement also inadvertently promote sensationalism and unsafe content. Key criticisms include:

- **Delayed removal of harmful content**.
- **Lack of transparency** in moderation decisions.
- **Weak age verification** systems.
- **Failure to prevent repeat offenders** from creating new accounts.

In *Reena Sharma v. Union of India* (2022), the Bombay High Court observed that "platforms cannot escape their duty by hiding behind technological limitations, especially when child safety is at stake.[30]

There is growing demand for **co-regulation**, where industry self-governance is monitored and enforced by a statutory regulatory body, possibly similar to the Telecom Regulatory Authority of India (TRAI) model.

6. Role of Parents, Schools, and Civil Society

While laws and platform policies are important, they alone cannot guarantee the online safety of children. The **ecosystem of protection** must include parents, educators, and civil society, who serve as the first line of defense. Digital literacy, awareness, and community engagement are essential for creating a safe and empowering online experience for children.

6.1 Role of Parents in Digital Guardianship

Parents play the most crucial role in protecting children online, but many are unaware of the specific risks or lack the digital skills to respond appropriately.

6.1.1 Digital Literacy and Awareness

A 2022 UNICEF India survey revealed that **only 37% of Indian parents** had adequate knowledge of the apps and platforms their children use.[31] Many lack the tools to guide online behavior, resulting in over-surveillance or complete neglect.

---

[28] https://indiankanoon.org/, *XYZ v. Meta Platforms Inc.*, Delhi High Court, 2023.

[29] Centre for Internet and Society. *Children Online: A Study on Abuse Reporting Mechanisms*, 2022.

[30] www.livelaw.in, *Reena Sharma v. Union of India*, Bombay High Court, 2022.

[31] www.unicef.org/india,UNICEF India. *Digital Literacy and Parental Engagement Survey*, 2022.

To address this:

- **Parental control tools** such as Google Family Link or Apple Screen Time should be used.
- Parents should **engage in regular conversations** about cyber risks like grooming, sextortion, and fake profiles.
- **Joint digital activities** (like co-watching or gaming) can help build trust and awareness.

6.1.2 Emotional Support and Trust

Creating an environment where children feel safe reporting cyber incidents is vital. Fear of punishment or judgment often causes children to stay silent even in cases of serious abuse.

According to Childline India, **70% of children who face online threats** do not disclose it to their parents.[32]

6.2 Role of Schools and Educational Institutions

Schools are key institutions in shaping children's digital behavior. With increasing access to school Wi-Fi and online learning tools, educators must incorporate online safety into the curriculum.

6.2.1 Digital Citizenship Education

Several CBSE-affiliated schools have introduced **Digital Citizenship and Internet Safety modules** as part of life skills education. These programs typically include:

- Identifying cyberbullying.
- Understanding digital footprints.
- Responsible use of social media.

6.2.2 Cyber Clubs and Safety Committees

Many progressive schools in metro cities have begun forming **Cyber Safety Clubs**, where students are trained to act as peer mentors. Safety committees consisting of teachers, counselors, and IT staff help monitor inappropriate use of school networks.

6.2.3 Collaboration with Law Enforcement

In cities like Bengaluru and Mumbai, schools collaborate with local police under **Cyber Safety Awareness Programs**, inviting officers for seminars and workshops on cyber laws and self-protection strategies.

Despite these efforts, implementation in **rural and underfunded schools remains negligible**, creating a digital divide in safety awareness.

6.3 Role of Civil Society and NGOs

Several non-governmental organizations have pioneered child-centric cyber safety initiatives in India.

6.3.1 Notable Initiatives

- **Childline India Foundation**: Operates a 24×7 helpline (1098) for children in distress, including online threats.
- **Cyber Peace Foundation**: Conducts national-level training, workshops, and research on digital safety for children.
- **Save the Children India**: Works in digital literacy and prevention of online sexual exploitation.In 2023, Cyber Peace Foundation partnered with the Government of Jharkhand to launch a **Digital Shakti 4.0 campaign**, aimed at educating girls about online rights and safety protocols.[33]

6.3.2 Capacity Building and Advocacy

NGOs often play a crucial role in:

- Conducting surveys and publishing safety reports.
- Building apps and tools for secure browsing.
- Training educators, police officers, and children.

However, many face **funding challenges** and rely on periodic government or CSR support.

6.4 Community and Peer Interventions

Children often turn to peers before adults when facing online troubles. Thus, promoting a culture of **peer responsibility** is essential:

- School initiatives like **"Cyber Buddies"** train older students to support and guide younger ones.
- Community workshops in residential societies help sensitize parents and children together.

[32] www.childlineindia.org.in,Childline India Foundation. *Annual Report on Child Safety 2022*.

[33] https://www.cyberpeace.org, Cyber Peace Foundation, *Digital Shakti Campaign Report 2023*.

- **Youth-led digital literacy projects** in urban slums and rural schools have emerged in states like Tamil Nadu and West Bengal.

Incorporating peer support mechanisms alongside parental and institutional efforts can build **resilient digital communities**.

6.5 Challenges in Offline Guardianship

Despite good intentions, several challenges persist:

- **Generational digital divide** between parents and children.
- Overdependence on schools without teacher training.
- Lack of cyber counselors in most Indian schools.
- **Stigma and taboo** around discussing topics like sextortion or grooming.

There is a pressing need for systemic support—including funding, curriculum redesign, and outreach programs—to empower offline stakeholders in protecting children online.

7. Policy Recommendations and Future Strategies

To effectively protect children from cybercrime on social media platforms, a **multi-pronged policy approach** is required. This section presents detailed recommendations at the legislative, institutional, technological, and social levels, emphasizing the need for **coordinated action** among government, platforms, educators, and families.

7.1 Legal and Regulatory Recommendations

7.1.1 Strengthen the IT Act and POCSO

The **Information Technology Act, 2000** and **POCSO Act, 2012** are foundational legal tools, but they require modernization:

- Introduce a **dedicated chapter on cybercrimes against children** in the IT Act.
- Define terms like **"online grooming"**, "cyberstalking of minors," and "deepfake pornography."
- Amend the POCSO Act to include **explicit provisions for online offenses**, such as digital coercion and sharing of morphed images.

7.1.2 Data Protection Legislation for Children

India's **Digital Personal Data Protection Act, 2023**[34] includes provisions for minors, but these need clarity:

- Mandate **explicit parental consent** for data collection from users below 18.
- Prohibit **behavioral advertising** and **data profiling** of children.
- Enforce **child-friendly privacy policies** written in simple language.

7.1.3 Fast-Track Cybercrime Units

- Establish **Child Cybercrime Investigation Units** in every district.
- Ensure these units are equipped with trained officers, forensic tools, and counselors.
- Set up **Fast Track Courts** for speedy trial of child-related cyber offenses.

7.1.4 Legal Accountability of Platforms

- Mandate **age verification using AI and KYC tools**.
- Hold platforms liable for failing to remove reported harmful content within 24 hours.
- Create a **statutory regulatory authority** for social media, with powers to audit safety systems.

7.2 Institutional and Educational Reforms

7.2.1 National Cyber Safety Curriculum

- Introduce a **mandatory digital safety curriculum** from primary school onwards.
- Include modules on fake news, cyber hygiene, sextortion, privacy, and reporting abuse.

7.2.2 School Cyber Counseling Units

- Appoint **cyber counselors** in schools, especially in urban and semi-urban areas.
- Conduct regular sessions with children, teachers, and parents.

7.2.3 Teacher Training and Incentivization

- Train teachers on **identifying behavioral changes** linked to cyber abuse.
- Offer **incentives and credits** for educators who complete cybersecurity and digital literacy courses.

7.3 Technological Innovations

7.3.1 Child-Centric Design Principles

- Platforms must embed **"safety by design"** principles, ensuring:
  - Age-appropriate content.
  - Opt-in features for discoverability.
  - Default private settings for children.

[34] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023*.

7.3.2 AI-Driven Safety Enhancements

- Use **AI to detect grooming behavior**, suspicious messages, and inappropriate content.
- Enable **predictive risk assessment tools** that alert moderators and parents in real time.

7.3.3 Verification and Transparency

- Introduce **verified accounts for educational or youth users**.
- Mandate **annual safety audits** and public reporting by platforms.

7.4. National Helpline and Support System

- Promote the **existing 1098 child helpline** as a cyber support line.
- Create a **24×7 emergency response portal** for reporting cyber threats affecting minors.
- Fund **mobile digital literacy vans** to visit rural schools and Panchayats.
- Partner with **Anganwadi workers** and **ASHA workers** to spread awareness in remote areas.
- Recognize "Cyber Safety Champions" at district and state levels to encourage participation.

7.5 International Best Practices to Emulate

India can learn from successful strategies implemented in other countries:

Country	Key Policy	Lessons for India
UK	Online Safety Act, 2023	Mandatory risk assessments by platforms; heavy fines.[35]
Australia	eSafety Commissioner	Independent body to enforce online child safety standards.[36]
US	COPPA (Children's Online Privacy Protection Act)	Parental consent before data collection from under-13s.[37]

India should explore the creation of an **Independent Child Online Safety Authority (ICOSA)** modeled on the eSafety Commissioner of Australia.

7.6 Need for Co-Regulation and Stakeholder Collaboration

Rather than relying solely on state or private action, India should move toward a **co-regulatory model** where:

- Social media platforms **collaborate with regulators** under formal codes of conduct.
- Government bodies provide **oversight and enforcement**.
- Civil society organizations ensure **transparency, education, and outreach**.

A unified **"National Child Cyber Safety Framework"** should be developed and monitored annually with inputs from ministries, platforms, educators, and NGOs.

8. Conclusion

The rapid evolution of digital technologies and the unprecedented rise in social media usage have created new opportunities and challenges for children. While platforms offer creative freedom, learning, and social interaction, they also expose minors to a wide array of cybercrimes—including grooming, cyberbullying, identity theft, and online sexual exploitation.

This research has shown that **cybercrime against children on social media platforms in India is a growing concern**, demanding urgent attention. Legal frameworks like the **Information Technology Act, 2000** and the **POCSO Act, 2012** provide a basic legal foundation, but they lack specificity and adaptability to meet the challenges of the digital era. Although the **Digital Personal Data Protection Act, 2023** offers some protections, a more robust and child-specific data regulation mechanism is needed.

Moreover, social media companies have a **shared responsibility** in safeguarding children but often fall short in areas like content moderation, age verification, and timely redressal of complaints. Their policies, although present, are inconsistently enforced, and technical tools such as AI-based moderation have not yet proven fully effective in the Indian context.

The role of **parents, schools, and civil society** is equally crucial. Offline guardianship through digital literacy, emotional support, and awareness education can prevent many online threats. However, disparities in digital access and awareness between urban and rural areas exacerbate vulnerabilities.

[35] www.gov.uk,Government of UK. *Online Safety Act*, 2023.

[36] www.esafety.gov.au,Office of the eSafety Commissioner, Australia. *Annual Report 2022–2023*.

[37] www.ftc.gov,U.S. Federal Trade Commission. *Children's Online Privacy Protection Rule (COPPA)*.

NGOs, youth volunteers, and community-led initiatives have shown promise in bridging this gap, but require sustained support and policy backing.

To ensure safer digital environments for children, a **comprehensive and multi-stakeholder approach** is essential. This includes:

- Legislative amendments to existing laws and introduction of child-focused online safety statutes.
- Co-regulation of social media platforms with clear enforcement mechanisms.
- Integration of digital safety into the national education policy and school curricula.
- Empowerment of civil society and parents through sustained awareness campaigns.
- Adoption of global best practices adapted to India's socio-cultural context.

Ultimately, protecting children online is not a task limited to any one entity. It requires **collective action** from government institutions, technology platforms, educators, parents, and the broader community. By acting now, India can not only curb cyber threats but also create a digitally safe and empowering environment for its future generations.

Reference

1. Ministry of Electronics and Information Technology. *Information Technology Act, 2000*.
2. Government of India. *Protection of Children from Sexual Offences Act, 2012*.
3. Ministry of Electronics and Information Technology. *Digital Personal Data Protection Act, 2023*.
4. UNICEF India. *Child Online Protection in India: Report*, 2022. www.unicef.org/india
5. Internet and Mobile Association of India. *Digital Adoption and Online Safety Report*, 2023.
6. Centre for Internet and Society. *Children Online: A Study on Abuse Reporting Mechanisms*, 2022.
7. Childline India Foundation. *Annual Report on Child Safety*, 2022. www.childlineindia.org.in
8. Cyber Peace Foundation. *Digital Shakti Campaign Report*, 2023. https://www.cyberpeace.org
9. Delhi High Court. *XYZ v. Meta Platforms Inc.*, 2023. www.IndianKanoon.com
10. Bombay High Court. *Reena Sharma v. Union of India*, 2022. www.livelaw.in
11. Government of UK. *Online Safety Act*, 2023. www.gov.uk
12. Office of the eSafety Commissioner, Australia. *Annual Report 2022–2023*. www.esafety.gov.au
13. U.S. Federal Trade Commission. *Children's Online Privacy Protection Rule (COPPA)*. www.ftc.gov
14. Karnika Seth, CYBER LAWS in the Information Technology ,Universal Law Publishing ,1 January 2009.
15. Bharatiya Nyaya Sanhita (BNS)2023, Taxmann Publications Private Limited, 22 November 2024
16. Talat Fatima ,Cyber Crimes, Bharat Law House.