

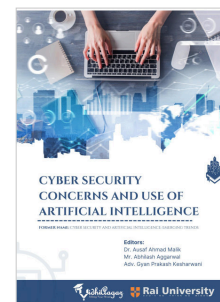
## CHAPTER 42

## Protecting the Unseen – Dealing with Cyber Crimes affecting Children

Vishakha Agarwal and Yogita C Javkar

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 354–359

ISBN 978-81-947620-5-8



## CITATIONS

BLUEBOOK (21ST ED.)

Vishakha Agarwal & Yogita C Javkar, *Protecting the Unseen – Dealing with Cyber Crimes affecting Children*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 354 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Vishakha Agarwal and Yogita C Javkar, 'Protecting the Unseen – Dealing with Cyber Crimes affecting Children' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 354.

CHICAGO (17TH ED.)

Agarwal, Vishakha, and Yogita C Javkar. "Protecting the Unseen – Dealing with Cyber Crimes affecting Children." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 354–359. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-42/>.

APA (7TH ED.)

Agarwal, V., & Javkar, Y. C. (2024). Protecting the unseen – dealing with cyber crimes affecting children. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 354–359). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-42/>

## SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-42/>

## RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

# PROTECTING THE UNSEEN – DEALING WITH CYBER CRIMES AFFECTING CHILDREN

Vishakha Agarwal<sup>78</sup> and Yogita C Javkar<sup>79</sup>

---

## **ABSTRACT**

*In recent years, digitalisation has become the new normal. From communicating and shopping to banking and other daily activities, everything happens at our fingertips. This increases the use of technology for all age groups, especially children. While digital platforms provide various opportunities, they also expose vulnerable groups to multiple types of cyber threats. Cyberbullying, internet exploitation, cyberstalking, identity theft, etc are some of the examples. With features like anonymity and the vast reach of the internet, it is easier to target children that are below the age of eighteen due to their lack of maturity level and awareness. Social media, gaming platforms, and artificial intelligence play a crucial role in cybercrimes as they expose children to privacy breaches, harassment, and inappropriate content which increases the need for improving security and parental supervision to protect children from exploitation. The existing literature shows that 36% of young people have experienced cyberbullying. In response, tech companies are enforcing strict content moderation policies, and schools are organizing anti-bullying programs to create awareness among students. However, the effectiveness of these measures in reducing cyberbullying remains a critical area for further research. Against this backdrop, the authors attempt to explore different cyber threats impacting children and highlight the connection between human rights and online safety. The paper is divided into two parts, Part one deals with the analysis of the various cyber threats faced by children, while part two offers suggestions that, if implemented, have the potential to significantly reduce the risks children face in the digital environment, promoting a balanced use of technology, and ensuring that children are better protected in the evolving digital environment.*

---

## **INTRODUCTION**

Digitalisation and the use of technology have become our backbone in today's generation. It has transformed the way we live, communicate, and interact. There is no doubt that it has brought various benefits and made our lives easy but it has created new opportunities for crime, especially towards vulnerable populations like children. Online offences targeting children have increased due to activities like cyberbullying online exploitation child pornography and identity theft. These threats attract children very easily due to their frequent use of social media platforms, online gaming, and educational websites which create an undetectable but significant danger. According to the National Crime Records Bureau (NCRB), 1,823 cases of cybercrimes against children were filed. It is essential to understand and fight back against these threats as children increasingly rely on the Internet for education, social interaction, and entertainment. There is a need for special attention because children are uniquely vulnerable in the digital space. Their innocence and lack of understanding of online dangers make them easy targets for cyber crimes. The introduction of stricter frameworks from legal, social, and technological sectors is essential to protect children online because traditional crime prevention methods are deficient in dealing with the challenges and anonymity of cyber crimes.

---

<sup>78</sup> Student at KLE Society's Law College, India.

<sup>79</sup> Student at KLE Society's Law College, India.

## **TYPES OF CYBER CRIMES AFFECTING CHILDREN**

It is vital to list down the following types of cybercrimes affecting children to understand the root cause of cyber-crimes affecting children –

a) **Cyberbullying:** Cyberbullying is one of the most common forms of cybercrime impacting children. Digital platforms are used to harass, threaten, or humiliate a child. Statistics say that in 2022, 158 cases of cyberbullying were filed. It is different from traditional bullying because it follows children into their homes through mobile devices and computers. The effects of cyberbullying are highly dangerous as it can cause emotional and psychological harm like depression, anxiety, and even suicidal thoughts.

b) **Child Pornography and Exploitation:** The production, distribution, and consumption of child sexual abuse material is one of the most heinous forms of cybercrime. 1,171 cases of cyber pornography were filed in 2022. Child pornography violates the rights and dignity of children and fosters a global market of exploitation. The prohibition of such crimes is difficult despite rigid laws in many countries due to the easy availability of such material in the online market.

c) **Online Predators:** Features provided by the internet like speed, convenience, anonymity, etc are often misused by online harassers to target children. They begin by gaining the trust of the victims by pretending to be individuals who share similar interests before engaging in exploitation. Children unknowingly involve in harmful activities, inappropriate conversations, send explicit content or get manipulated for sexual exploitation leading to psychological issues like trauma, distrust, emotional damage, etc.

d) **Identity Theft and Data Privacy:** Children below the age of eighteen years are unaware of the nature and consequences of the activities they are involved in. Their active involvement in social media and gaming platforms is prominent daily. This allows them to share their personal information without being aware of the risks like data breaches and exploitation. Criminals can use a minor's identity to commit fraud, misuse bank statements, and participate in illegal activities resulting in long-term consequences affecting the child's future.

## **LEGAL FRAMEWORK FOR CHILD PROTECTION**

It is essential to form a vigorous legal structure for child protection against cybercrime in the digital environment. This is because there was an overall increase of 8.73% in crimes against children which sums up to 1,62,449 cases in 2020. Let's have a look at the following elements and angles of the legal system in different regions –

i) **Internationally,** the United Nations Convention on the Rights of the Child (UNCRC) stresses the protection of children from exploitation and abuse in digital spaces. Optional Protocol on the Sales of Children, Child Prostitution, and Child Pornography tackles issues related to online child exploitation. Council of Europe's Convention on Cybercrime offers a framework for international cooperation in battling cybercrime offences against children.

ii) Most countries have introduced laws to protect children from cyber crimes. Laws like Child Protection Laws, Data Protection and Privacy Laws, and Cybercrime Laws are some examples that protect children from abuse, personal data and privacy online, and criminalize activities like online harassment, child pornography, and identity theft. Moreover, the Children's Online Privacy Protection Act (COPPA) in the United States demands that websites and online services must obtain parental consent before collecting personal information from children below 13. The Online Safety Bill in the United Kingdom enforces stricter rules and regulations on social media platforms to confirm child safety. The Protection of Children from Sexual Offences (POSCO) Act in India criminalizes the production, distribution, and possession of Child Sexual Abuse Material (CSAM). However, many nations lack in having exhaustive laws handling all types of cyber-crimes targeting children. Therefore, the legal system for child protection against cybercrime must be diverse including international standards, national legislation, and collaboration among various stakeholders so that a safer digital environment for children can be created.

### **LANDMARK CASES ADDRESSING CYBERCRIME AGAINST CHILDREN**

State of Tamil Nadu v. K. Ramasamy (2019) in India dealt with issues of child pornography and supported the importance of legal provisions of Section 67B under the Information Technology Act, 2000 which prohibits the publishing and transmitting of child pornography. United States v. C.M. (2019) in the United States involved a minor who was accused of sending nude images of herself to peers where the court made judgements on the challenges relating to sexting among children handling issues of consent and child pornography laws. In R v. T (2007) in the United Kingdom the court's decisions were made on the use of online chat rooms to groom children for sexual exploitation which led to making legal guidelines for prosecuting digital sexual crimes involving minors. Similarly, various cases in Australia, Canada, and the European Union made a mark on issues relating to child pornography, child exploitation, etc.

### **TECHNOLOGICAL SOLUTIONS FOR PREVENTION**

To prevent these cyber-crimes against children, it is necessary to make solutions in the technological aspects i.e., imposing parental control software for monitoring and restricting children's online activities, using the right amount of artificial intelligence and machine learning to identify and oppose cyber crimes relating to children, providing encryption and data privacy tools ensuring that sensible information like locations, identities, and images are not easily accessible to cyber bullies. Moreover, software like blockchain technologies, cyberbullying detection and prevention tools, tracking tools, VPNs, and digital footprint management tools must be introduced to verify identities of users in online environments, offer real-time monitoring of social media interactions, allow parents/guardians to track their child's real-time location, to create secure and encrypted connections for children, and help manage and reduce the amount of data that apps and websites collect from the users.

### **ROLE OF EDUCATIONAL INSTITUTIONS AND PARENTS**

In addition to technological solutions, educational institutions and parents also play a vital role in a child's life that can help prevent and address cyber crimes against children. Their combination can form

a protective environment that helps children develop skills and awareness important to guide digital world safety.

Educational institutions must incorporate cyber safety into their programme so that responsible internet use, identifying cyber threats, and protecting personal data can be taught to children. Workshops and seminars must be conducted by professionals that can raise awareness among students, teachers, and parents about the risks of cybercrime. Students must be taught about these crimes age-appropriately i.e., younger students can learn about stranger danger online and older students can learn about phishing, sexting, and privacy settings. Schools must establish clear policies and protocols like anti-cyberbullying policies, acceptable use policies for school computers, mobile devices, and internet access, structured reporting system for cybercrime incidents to spread awareness of safe and appropriate online behaviour. Along with the students, teachers and counsellors must be trained on cyber safety so that they can identify signs of cyberbullying, online harassment, and online harassers and most essentially identify vulnerable students who may be victims of cybercrime. Schools must provide a safe online learning environment i.e., monitoring and ed-tech tools that can block harmful content, detect potential cyber threats, and recognise theft or exploitation of personal data. Partnerships with law enforcement and cybersecurity experts are another step that schools can take to update emerging cyber threats develop protocols and help students and parents to understand the real-world impact of cybercrime.

Children spend most of their time with parents at home which makes them responsible as well to preventing their child from cyber-crimes. Their active participation in online activities like supervising their children's online behaviour, the apps they use, the websites they visit, and the people they communicate with online, creates open lines of communication and modelling good digital behaviour. The right way of using parental control tools must be used to block harmful content, limit screen time, and monitor their children's online interactions. Parents must teach their children to adjust privacy settings to protect their personal information to reduce online crimes. Furthermore, parents must learn to educate their children about online safety like teaching how to behave respectfully online, educate their children about common online threats and predators, and explain the threat of sharing personal information, photos, or videos online. They must set clear instructions regarding screen time, social media use, and use of the internet. Most importantly, parents must create an atmosphere with their children in such a way that can foster trust among themselves. This will encourage honest communication and prevent cyberbullying or suspicious activities. Parents shouldn't fear reporting any cybercrime incidents to either schools, law enforcement, or appropriate authorities.

Therefore, their respective roles can help prevent cybercrime against children by offering education, supervision, and the right technological tools.

### **PSYCHOLOGICAL IMPACT ON CHILDREN**

Numerous types of cyber-crimes against children including cyberbullying, online grooming, exploitation, and exposure to harmful content can result in intense psychological impacts. Children below the age of eighteen experience feelings of fear, shame, and helplessness, leading to anxiety, depression, and social withdrawal especially because minors are innocent, emotional and sensitive.

Children are most of the time targeted due to humiliation and isolation where harmful messages or images can be shared widely and permanently. Activities like online exploitation involving child pornography can extremely affect a child's self-esteem leading towards trauma, trust issues, and long-term emotional scars. These psychological impacts can affect a child's academic performance, relationships, and normal developmental milestones, requiring professional counselling and family support to help children process the emotional damage and recover their sense of safety.

### **CHALLENGES IN LAW ENFORCEMENT**

The legal system comes across many challenges while focusing on cyber crimes against children. Firstly, jurisdictional complexity is one of the most prominent obstacles because cyber-crimes commonly cross national borders wherein it is difficult to determine applicable laws or to coordinate with international investigations. There are complications in tracking and identifying online predators due to the features provided by the internet. Digital shreds of evidence are temporary as they can be deleted or edited easily which makes it impossible to punish the offenders. Moreover, limited resources and technical expertise within law enforcement agencies further hinder their ability to stay ahead of constantly evolving cyber threats. Lack of specialized tools or training vital to confront cybercriminals and delays in adapting to new technologies allow offenders to exploit gaps in execution. There is an increasing need for public-private sector collaboration because private tech companies control most of the data needed for investigations. Altogether, these challenges create substantial barriers to effectively fighting cyber-crimes against children.

### **RECOMMENDATIONS FOR FUTURE ACTION**

Several key actions must be taken to protect children from cyber-crimes effectively. International cooperation should be strengthened to handle jurisdictional challenges and improve the prosecution of offenders. Technological solutions, including advanced parental controls, AI-based monitoring systems, and encryption techniques should be stronger and implemented worldwide to discover and prevent harmful activities online. Schools must introduce detailed cyber safety education into their syllabus where both students and teachers are guided accordingly. In addition to that, parents also must receive guidance on how to foster safe online habits at home. There must be stronger enforcement of existing laws with necessary amendments and updating legislation to address emerging dangers and close any legal loopholes. Law enforcement agencies must be provided with sufficient training and resources to effectively combat cyber-crimes, while working closely with the private sector, particularly tech companies, to track and remove harmful content. Increased psychological support and counselling should be available to children who fall victim to cyber crimes, as the emotional toll can be significant. Developing specialized recovery programs will help ensure that these children can regain their mental and emotional well-being after such traumatic experiences. Implementing these recommendations is crucial because reports say that 445 crimes take place in a day which means 18 incidents per hour.

### **CONCLUSION**

Cybercrime against vulnerable groups especially children is an increasing and concerning issue. Children are subjected to various threats in the digital world due to activities like cyberbullying and online exploitation. There is a need for rigid and strict improvement and innovation in fighting these crimes because protection from legal frameworks, technological tools, and educational programs contain loopholes. Every sector such as government, legal systems, private bodies, schools, parents, etc must come together, and collaborate to ensure the safety of children in cyberspace.

\*\*\*\*\*