

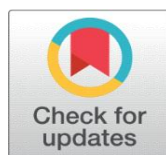
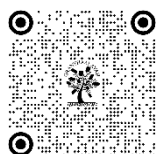


SAFEGUARDING CHILDREN'S DATA IN THE DIGITAL AGE: A LEGAL APPROACH TO PREVENT CYBERATTACKS AND CHILD SEXUAL ABUSE

Sumedha Gupta ¹, Dr. Sandhya Kumari ²

¹ PhD Research Scholar School of Law, Galgotias University, Greater Noida, India

² PhD Guide and Professor school of Law, Galgotias University, Greater Noida, India



Corresponding Author

Sumedha Gupta,
adv.sumedhagupta@gmail.com

DOI
[10.29121/shodhkosh.v5.i5.2024.1590](https://doi.org/10.29121/shodhkosh.v5.i5.2024.1590)

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2024 The Author(s). This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.



ABSTRACT

The growth of digital technologies and online platforms has dramatically increased the risk of children becoming victims of sexual abuse. Cybercriminals often abuse children's personal information, such as their name, age, location, and online activities, to identify and exploit them. However, this digital revolution has also led to increased risks, including the vulnerability of children's data to cybersecurity attacks. One of the most concerning consequences of such attacks is facilitating child sexual abuse. Therefore, protecting children's data is essential in preventing child sexual abuse. In this background based on this hypothesis, this paper focuses on the legal approach to protect the vulnerability of children's data from cybersecurity attacks. The paper analysis the legal frameworks and guidelines developed by the Indian government to safeguard the personal data of children. Further, it would identify the current gaps in the legal framework and emphasise the need for further improvements towards strengthening the data protection of children. Moreover, the paper explores the role of technology in protecting children's data, including data encryption, secure data storage, access controls, and monitoring systems and also analyses the challenges associated with implementing these technological solutions. Finally, the paper offers suggestions for policymakers, legal practitioners, and technology professionals to protect children's data from cyberattacks, thereby preventing child sexual abuse.

Keywords: Cybersecurity, Children's Data Protection, Child Sexual Abuse, Legal Framework, Technology

1. INTRODUCTION

Internet has been a worldwide sensation since its inception, following COVID-19 and the lockdown that the virus caused, there was a significant change in the average amount of screen time spent by each user. Children, particularly school-aged children, have been required to adjust to the many changes brought about by the pandemic. One of these changes has been an increase in children's usage of the internet for a variety of reasons, including education and entertainment, to name a few. Since its inception, the internet has been a phenomenon that can be observed all over the world. Despite the fact that the positives far outweigh the negatives, it is a fact that the internet has become a breeding ground for a large number of people

who engage in abusive behaviour and criminal activity. When an individual uses the internet, the cyber security of that individual is perpetually put at risk. It is quite common for there to be many instances of data breaches and personal information being compromised, despite the fact that many internet-based platforms frequently guarantee that the user's data and chats are encrypted end-to-end. One of the most significant reasons for concern in relation to these data breaches and other types of cyber security threats is the fact that the majority of the time, data pertaining to children are exposed, and very frequently, the children are abused online as a direct result of their personal data being exposed. This is one of the most significant causes for concern because it is one of the most significant causes for concern in relation to these data breaches and other types of cyber security threats.

Even though there are pieces of legislation in place, such as the Information Technology Act of 2000 and other pieces of legislation that are similar, there are still a number of modifications that need to be made to the current legal landscape of Indian jurisprudence in order to make the laws more proactive and stringent. These modifications need to be made to the current legal landscape of Indian jurisprudence in order to make the laws more proactive and stringent. These adjustments are reflected in the modern legal landscape in various forms.

This article addresses a variety of concerns and potential risks that are connected to the practice of allowing children to use the internet. It also discusses the ways in which the internet is used as a platform to abuse children, as well as the ways in which their personal information is used for unethical practices such as child pornography and child prostitution. In addition, it looks at the ways in which children's personal information is used for unethical practices.

2. UNDERSTANDING CYBERSECURITY ATTACKS ON CHILDREN

In today's modern world, ensuring the safety of networks against malicious cyberattacks is one of the most essential things that can be done. There are approximately 4.66 billion people using the internet right now, which is equivalent to approximately 60 percent of the total population of the world, and these numbers continue to rise on a daily basis. The most recent estimates put the number of people using the internet at approximately 4.66 billion. As was mentioned earlier, the internet has developed into a fundamental resource comparable to clean air and water, and the Indian Supreme Court (hereinafter referred to as the SC) has issued a number of judgments in which it has stated that access to the internet is a fundamental right that falls under the purview of the constitution.

An antivirus program is typically installed by a user with the promise that the user's data will be protected by the program; however, this is not the case. As a result of advances in technology, cyberattacks have become increasingly common, and children, who are the most defenceless demographic when it comes to this type of attack, are extremely susceptible to it. The term "cybersecurity" refers to the practice of defending computer systems, mobile phone networks, and other types of electronic infrastructure against intrusion attempts. As a result, it is of the utmost importance to have a conversation about the current state of cyber security and the susceptibility of children to the many different types of cyberattacks. However, cyberattacks are capable of having a significant impact on a person because they can cause both mental and physical distress, and they can even lead to more serious offenses, such as sexual abuse and blackmail. Cyberattacks are not given the same level of respect as other types of criminal activity, such as robbery or murder. Children, due to their young age, do not typically understand the consequences of

engaging with people online. This is especially true when it comes to cyberbullying. This means that it may lead to the sharing of personal photos, videos, and important details with complete strangers on the internet, which could be used to the person's detriment if the information was in the wrong hands.

We would now be discussing about the various cybersecurity attacks and threats that the children are vulnerable to-

Cyberbullying:

This kind of cyberattack is by far the most prevalent, and almost anyone who uses the internet could be at risk of falling victim to it. The extent of damage that can be caused by cyberbullying can vary greatly across a wide spectrum of degrees, just as it can manifest itself in a wide variety of different ways. According to the United Nations Children's Fund (UNICEF), the term "cyberbullying" refers to any form of bullying that takes place through the utilization of digital technology. There is a chance that it will take place on mobile phones, messaging systems, gaming platforms, or websites related to social media. People are singled out for harassment, humiliation, or intimidation when they are subjected to repeated behaviors that are designed to achieve one of these goals. This can take the form of verbal abuse, physical assault, or social exclusion. Repeated instances of cyberbullying can have a detrimental effect not only on a person's mental and physical health but also on their emotional well-being. This is true whether the bullying is directed at an individual or a group.

Doxing:

Despite the fact that it is one of the most serious types of online attack that could happen to anyone, this particular form of cyberattack is most likely to affect younger people, particularly adolescents and children. This is true despite the fact that it is one of the most common forms of cyberattack. Doxing is the act of obtaining or compiling private information about another individual and then publishing it on the internet without that person's knowledge or consent. Taking revenge on another person is typically the motivation behind this particular form of bullying, which is directed at that person. Information can be obtained through a variety of channels, including social media platforms like Facebook and Twitter, personal accounts, and even computer hacking. By using doxing, one is able to achieve a variety of goals, including coercion, online shaming, extortion, and even vigilante justice. These are just some of the primary goals that can be achieved.

Sextortion:

One of the many severe cyberattacks that has also been linked to the abuse of children is this one. Attacks of this nature frequently target children because of their tender years and high susceptibility to trauma. A sextortion scam is essentially a threat that is given to the victim by the perpetrator in which the perpetrator blackmails the victim for money in which the perpetrator may claim to have a revealing picture of the child that will be shared if the victim does not share more photographs, it may also turn into a financial sextortion in which money or other types of gifts are demanded from the child.

Legal frameworks and guidelines developed by the Indian government to safeguard the personal data of children

Though as we have discussed by now, there have been some pro-active legislations in the direction of child safety and preventing their abuse on the internet, still we are a long way to go. Some of the major legislations in this direction and their loopholes would be discussed in this section, this includes the Information Technology Act, 2000, various sections of the Indian Penal Code, 1860 and

Protection of Children from Sexual Offences Act, 2012. These legislations and their relevant sections would be discussed henceforth-

Information Technology Act, 2000:

This legislation has proven to be a ground-breaking piece of legislation, and it was absolutely necessary in light of the shifting political climate in India, in which the technological landscape was evolving and it was essential to protect the rights and interests of individuals while they were using the internet. The publication and transmission of child pornographic material or any other form of offensive content, as well as content representing children engaged in sexual behaviour, in any form of electronic media is illegal, as stated in Section-67B of the Act. This includes content depicting children engaging in sexual activity. Section 67B of the Act outlines the various punishments that may be imposed for the same infraction. Other clauses include the following: a) It is a breach of a person's right to privacy to publish or transmit photos of that person's private life, regardless of whether or not that person has granted permission for the use of their image. This provision applies even if the individual has provided permission for the use of their image. b) creating a connection with a kid with the intention of sexually exploiting the child in a future relationship by making use of the child's personal information in order to facilitate the connection. c) unlawful access to computers or any other electronic devices can result in a breach of privacy, the theft of data, tampering with electronic devices, the corruption of the device through the introduction of a virus, and the damage of a computer program. These issues can also be caused by unlawful access to electronic devices in general. This act is only directly directed at the children; nevertheless, it can be directed against any individual who, in turn, includes children within their sphere of influence. Children are the only targets of this act. Both dishonestly accepting any sort of electronic device impersonation and performing identity theft by using another person's password or electronic signature without their consent are instances of this type of behavior. Identity theft can be committed by using another person's password or electronic signature without their permission. d) An intrusion of any kind on the right of children to have their privacy respected.

POCSO Act, 2012:

This act was enacted to protect children from all types of sexual offences as the erstwhile laws were not enough to deal with instances of child abuse and the quantum of punishment was not enough to deal with the gravity of the crime. The relevant provisions of the POCSO act are discussed below- Section 2(da) of the Act defines "child pornography", as "any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer-generated image indistinguishable from an actual child, and image created, adapted, or modified, but appear to depict a child;"

Section 11 of the POCSO Act provides instances for sexual harassment. The following are some examples that involve electronic media:

- 1) It is considered sexual harassment of a child when an adult act with the intent to have sexual relations with a child and then displays pornographic material to the child using any form of electronic media.
- 2) It is considered sexual harassment when an adult makes repeated contact with a child through any form of electronic communication.
- 3) A person who is guilty of sexual harassment, if they threaten a child through any form of electronic communication to use any body part of the child or to involve the child in a sexual act, regardless of whether or not the act was real.

- 4) Lures a child for the purpose of engaging in pornographic activity.

The Indian Penal Code, 1860:

Offenses such as criminal intimidation, hate speech, and defamation that are committed online fall under the purview of the Indian Penal Code.

- 1) The expression of hatred is regulated by Indian Penal Code section 153 A. If anyone commits an act that leads to the promotion of animosity between different groups on different grounds and that is detrimental to the upkeep of harmony, then that person will be held accountable.
- 2) The offense of cheating by impersonation is addressed by Section 419 of the IPC. Any person who commits the offense of cheating by impersonation will be punished with imprisonment for a term that may extend to three years or a fine, or both, according to the provisions of the section.
- 3) The issue of defamation is addressed in Section 500. Any person who commits the crime of defamation will be punished with simple imprisonment for a term that could last up to two years, a fine, or both of these options, depending on the severity of the crime.
- 4) Intimidation of a witness or victim is the subject of Section 506. A person who commits the crime of criminal intimidation will be punished with imprisonment for a term that could last up to two years, a fine, or both of these options, depending on the severity of the crime.
- 5) Obscene material can't be owned, sold, or otherwise dealt with legally thanks to Section 292.

The Indian Penal Code addresses these issues in a general sense rather than focusing specifically on children. However, this can be applied even in situations where the aforementioned offenses were committed against children.

Data Protection Bill, 2021

The bill includes a variety of protections to ensure the confidentiality of the personal information of children. The requirement that individuals must be 18 years old before giving their consent is among the most crucial provisions. According to the provisions of the bill, in order to process the personal information of a child, a data fiduciary must first obtain consent from the child's legal guardians. In addition to this recommendation, it suggests that any data fiduciary that deals exclusively with children should be required to register with the relevant data protection authority. The processing of children's data and the provision of services to the children are both considered to be qualifying factors for the determination of a significant data fiduciary. Additional responsibilities are outlined in the bill, and data fiduciaries with significant responsibility must comply with them. It is against the law for data fiduciaries to monitor or track the data of children, and it is also against the law for them to process personal data in a way that could put the children in danger.

3. CONCLUSIONS AND SUGGESTIONS

In the digital age, where children are increasingly exposed to online platforms and activities, protecting children's data from cybersecurity attacks is critical. This project delves into the critical issue of protecting children's data in order to prevent child sexual abuse, taking a legal approach to address this complex and evolving challenge.

These cyber-attacks take advantage of vulnerabilities in children's online activities, such as social media, online gaming, and e-learning platforms.

Cybersecurity breaches affecting children's data have far-reaching consequences, affecting their privacy, psychological well-being, and overall safety.

Our review of existing legal frameworks revealed a patchwork of international conventions, treaties, and national laws aimed at protecting the rights and data of children. While these legal measures have made significant progress, there are still several obstacles and gaps that must be addressed. Complex jurisdictional issues, the rapid pace of technological advancements, and a lack of harmonization between international and national laws all pose barriers to effective protection.

We propose a multifaceted approach to strengthening legal frameworks for enhanced protection. Integrating technological solutions, such as encryption and advanced authentication methods, can help to improve cybersecurity. Combating cross-border cyber threats that target children requires international cooperation and collaboration among nations. It is critical to equip law enforcement agencies with the tools they need to investigate and prosecute cybercrimes. Furthermore, educating parents, educators, and children about online risks and responsible internet use will aid in the creation of a safer digital environment.

We have emphasized the ethical considerations associated with the protection of children's data throughout this project. To respect children's rights and ensure their well-being, it is critical to balance privacy and security while obtaining informed consent for data collection. Promoting digital literacy among children and adults is critical to fostering an online safety culture.

To summarize, protecting children's data from cybersecurity attacks in order to prevent child sexual abuse necessitates a comprehensive and evolving legal strategy. We can create a safer digital landscape for our children by combining legal measures with technological advancements, ethical considerations, and broad-based collaboration. This project emphasizes the importance of proactive efforts to protect the digital well-being of our society's most vulnerable members - our children. Only by working together can we create a safe and nurturing digital environment that safeguards their innocence, privacy, and future.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

- Kumar, S., 2023. Cyber Crimes Against Children in Virtual World an Empirical Study with Specific Reference to Kangra District Himachal Pradesh. <https://www.sciencedirect.com/science/article/pii/S240584402203777X> accessed 28 July 2023.
- Dombrowski, S.C., LeMasney, J.W., Ahia, C.E. and Dickson, S.A., 2004. Protecting children from online sexual predators: technological, psychoeducational, and legal considerations. *Professional Psychology : Research and Practice*, 35(1), p.65.
- The Information Technology Act, 2000
- Broadhurst, R., 2019. Child sex abuse images and exploitation materials. Roderic Broadhurst, *Child Sex Abuse Images and Exploitation Materials*, in Roger Leukfeldt & Thomas Holt, Eds. *Cybercrime : the human factor*, Routledge.

Wittes, B., Poplin, C., Jurecic, Q. and Spera, C., 2016. Sextortion: Cybersecurity, teenagers, and remote sexual assault. Center for Technology Innovation at Brookings, pp.1-47.

Section 67B, Information Technology Act, 2000.

Ibid 8.

Section 2(da), Protection of Children from Sexual Offences Act, 2012.

Section- 153A, Indian Penal Code, 1860.

Section- 419, Indian Penal Code, 1860.

Section- 500, Indian Penal Code, 1860.

Section- 506, Indian Penal Code, 1860.

Section- 292, Indian Penal Code, 1860.