International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Cyber Safety and Children: A Digital Analysis with Special Reference to Rethinking Digital Protections in a Vulnerable Online Age

Dr. Chandan Kumar Sinha

PhD in Faculty of Social Science
Email: *cksinhahrm[at]gmail.com*

Abstract: ***This paper is intended to delve into the intricacies of the interaction between technology and children. The focus is on giving the reader a better and more nuanced understanding of how cybersecurity has a bigger role to play than mere protection of privacy and data. Children of younger age are the most vulnerable population on the internet filled with anonymous users whose identity is unknown. Children often face Instances of extortion, cyberbullying, and exposure to inappropriate content which may affect their mental or physical well-being, putting the future of society at threat. The first part of the paper contains an analysis of the impact of the internet and social media on children. This part is aimed at explaining to the reader how vulnerable populations, especially children, are the vulnerable victims of cybercrimes. The second part of the paper focuses on detailing various cybercrimes that impact children's safety and well-being online. The third part of the paper is aimed at providing a critical overview of the political and legal position in India regarding the Internet and child protection. The fourth part of the paper will try to assess the effectiveness and impact of bans on the use of social media for children. The final part of the paper is aimed at giving a potential solution to tackle this internet threat to protect our children and preserve their childhood for a better future for society.***

Keywords: Child cybersecurity, online safety, Cyber-bullying, online child sexual exploitation, Cyber-grooming, Blanket Ban, Identity theft, Malware, Phishing Attack, Parental control, Digital literacy, Digital Footprints. Cyberbullying, internet laws in India, and digital well-being

1. Introduction

Freedom of speech and expression is a fundamental human right. According to Article 19 of the Universal Declaration of Human Rights, everyone has the basic right to freedom of opinion and expression; this right includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[1] This right is also really well recognized by the Indian constitution, Article 19, and time to time upheld by the honourable Supreme Court as inviolable.[2] As the digital space expands and more people exercise their right to free speech online, it becomes equally important to address the rising threats in cyberspace that can hinder this fundamental freedom. India has the second-largest online community in the world, with over 560 million internet users. This number is expected to grow to 970 million by 2025. With so many people online, the risk of cybercrimes like fraud, threats, and blackmail is also increasing. The anonymity of cyberspace has emboldened individuals to engage in activities they might avoid in real-world interactions.[3] Due to this reason, individuals with ulterior motives or out of ignorance do such things which they would not have done if they lacked anonymity. This rising digital engagement has made children, with their limited understanding of online risks, particularly vulnerable to cybercrimes. After the pandemic, the number of young children using the internet has substantially increased because of the necessity of attending classes online, and for entertainment purposes. This advent of digital inclusion, especially post-pandemic, has rampantly aggravated the situation of cybercrimes. Children due to their limited knowledge of the world and innocence, are most vulnerable to cybercrimes. The invasive methods marketers use to gather personal information from children have raised serious concerns about data privacy and security. These concerns focus on whether children fully understand and can consent to such data collection, highlighting the importance of parental approval and supervision, especially for the youngest internet users.[4]

According to the National Crime Prevention Counsel, 43 per cent of teens have been victims of cyberbullying, but many are too ashamed or embarrassed to report the incidents to their parents or other authorities.[5] Children are spending more time online than ever before. And they're getting there sooner. Around the world, a child goes online for the first time every half second. Understanding the internet's impact on children is crucial for shaping stronger laws, raising awareness, and

[1] Humanrights.com. 2022. Article 19 of the Universal Declaration of Human Rights. [online] Available at: <https://www.humanrights.com/course/lesson/articles-19-25/read-article-19.html> [Accessed 25 July 2022].
[2] The constitution of India (1950), Art. 19
[3] Shariff, S., 2008. '*Cyber-bullying: Issues and solutions for the school, the classroom and the home.' Routledge.*
[4] Sonia Livingstone, M. Stoilova, and R. Nandagiri, 'Children's data and privacy online: Growing up in a digital age. An evidence review' (2019) London: London School of Economics and Political Science. (p. 4)
[5] Archive.ncpc.org. n.d. [online] Available at: <http://archive.ncpc.org/resources/files/pdf/bullying/Teens%20and%20Cyberbullying%20Research%20Study.pdf> [Accessed 5 Feb 2025].

providing targeted education to safeguard their online experiences.

2. How the Internet Affecting Your Child

What happens online reflects the realities children face every day – at home, at school and in their wider communities.[6] Cyberbullying and other forms of peer-to-peer violence can affect young people each time they log in to social media or instant messaging platforms. When browsing the internet, children may be exposed to hate speech and violent content – including messages that incite self-harm and even suicide.[7]

What are the most common types of threats which a child faces:

Cyber Grooming: Cyber grooming is a cyber threat that is faced by children across the globe. Essentially, this is a threat in which an individual attempts to develop an emotional connection with a child, through cyber means. The individuals practice this through various cyber means like social media, online gaming websites etc. The individual pretends to be a child and this leads to the children trusting them eventually. After some time, when the trust between the child and the imposter gets built, the imposter gets the ability to take advantage of the child and use the child accordingly.[8]

Cyber Bullying: As per 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. Examples include: (a) spreading lies about or posting embarrassing photos or videos of someone on social media. (b) Sending hurtful, abusive or threatening messages, images or videos via messaging platforms. (c) Impersonating someone and sending mean messages to others on their behalf or through fake accounts. Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse.[9]

Exposure to inappropriate content: While the internet stimulates social connection, participation and creativity, it also facilitates the spread of inappropriate content, such as hate messages and images of violence, which can negatively affect children's identity, sense of self-worth and view of the world. This reinforces the urgency of developing efficient protection measures in a world where online hate and violence are becoming a global problem (United Nations Children's Fund, 2017).[10] This inappropriate content also includes adult content which may affect the psychological well-being of a child. Access to these content at an early stage may lead the child to adopt abnormal behaviour and may cause depression, or may increase their tendency to commit crimes or suicide.

Data Privacy and Identity theft: There is also a huge possibility of children sharing their personal information such as their full name, addresses, school details, parent's occupation or card details, making them suspectable of identity theft and fraud. Studies suggest that the mediated nature of social network communication facilitates greater self-disclosure of personal information than face-to-face interaction.[11] Cybercriminals can use this information for various malicious activities, such as financial fraud or phishing scams.

Summing up, the internet plays a crucial role in a child's life today but also exposes them to significant risks. If the dangers of the internet and social media are not mitigated it can lead to psychological and physical harm to children of young age. Consistent exposure to harmful content and cyberbullying may cause emotional instability and may influence them to commit crimes. Therefore, the protection of children in this internet era is a significant task for the parents, government and tech industries.

What are the legal safeguards: Analysis of Indian law

The IPC[12] contains general provisions against harassment, defamation, and blackmail, these are not designed to address the online nature of child abuse. The IPC does not account for newer forms of child exploitation, such as cyberbullying, gaming platform abuse, or dark web trafficking. The act was originally enacted in the 1860s, and even the amendments introduced in the laws are too slow to match the pace with the evolving nature of the internet and cybercrimes. Punishments are often too lenient to deter repeat offenders, and cases take years to resolve in courts. To tackle the growing problem of cybercrimes, the Indian Parliament introduced the Information Technology Act, of 2000. This law was created to address various cyber-related issues and regulate activities in the digital world. However the act is concerned with objective substantive law, it does not have special emphasis on the need to protect children on the Internet. However, with some amendments, the legislators extended some provisions to address the problem of child abuse. Section 67B of the said act punishes an individual for publishing or transmitting materials which depict a child in a sexually explicit act.[13] Apart from the IT Act, 2000 and its amendment, the POCSO Act, 2012 (Prevention of Children from sexual offences) also

[6] Protecting Children Online, UNICEF. < https://www.unicef.org/protection/violence-against-children-online> [Accessed on 5 Feb 2025]

[7] Ibid.

[8] Dr. Nagarathna A., Jay Bhaskar Sharma, Sparsh Sharma. Children and Child Safety-an-e-book. Advance Centre for Research, Development and Training in Cyber Laws and Forensics, National law school of India university Bangalore. (p. 4)

[9] Unicef.org. n.d. 'Cyberbullying: What is it and how to stop it.' Available at: <https://www.unicef.org/end- violence/how-to-stop-cyberbullying> [Accessed 5 Feb 2022].

[10] Daniel Kardefelt Winthera , Mariya Stoilovab , Moritz Büchia , Rogers Twesigyea , David Smahelc , Marie Bedrosovác , Nikol Kvardovác , Sonia Livingstoneb, Children's exposure to hate messages and violent images online, UNICEF. https://www.unicef.org/innocenti/media/2621/file/UNICEF-Children-Exposure-Hate-Violence-Online.pdf [Accessed on 7th feb 2025]

[11] Sonia Livingstone, M. Stoilova, and R. Nandagiri, 'Children's data and privacy online: Growing up in a digital age. An evidence review' (2019) London: London School of Economics and Political Science. (p. 11)

[12] Indian penal code, 1860

[13] IT (Amendment) Act 2008, s 67B

specifically entails a provision for the protection of children from their malicious usage by perpetrators for pornographic purposes in the digital environment. The POCSO Act is India's most robust law for child sexual abuse but is largely designed for offline crimes. Section 13 of the act says that using a child in any form of media for sexual gratification, including indecent representation or involvement in sexual acts, is a punishable offence.[14] There are only a few provision which talks about the sexual abuse of children online. Lawmakers should not under-evaluate the impact and potential of the internet in children's sexual abuse given the weak internet protection regime in India.

Since the introduction of the IT Act, of 2000, cybercrime cases have increased, which is expected as more people use the internet. However, despite the law being strong at the time, the rapid growth of digital technology, including Artificial Intelligence and the Internet of Things, has allowed criminals to find new ways to escape punishment.[15] The rapid growth of digital technologies has left a gap in laws, services, and education to ensure safe and positive online experiences for children. As a result, children can be at risk of serious harm, like exploitation, trafficking, cyberbullying, and invasion of their privacy.[16] The lack of updated laws to regulate the evolving cyber world has made children even more vulnerable to online threats. After the COVID-19 pandemic, internet usage surged, increasing the risk of cybercrimes against children, such as online exploitation, cyberbullying, and abuse. The rise in cyberattacks, like the "Shadow Pad" malware attack on Mumbai's power grid in 2020, highlights major gaps in cybersecurity, showing the urgent need for stronger protections, especially for children in the digital space.

Is Banning Access A Solution: Australian case study

Recently, the Australian government banned the use of social media for children below the age of 16 years.[17] The ban was met with mixed responses from the parents and media houses. The ban is considered to be one of the strictest laws in recent years concerning the usage of the internet. Prime Minister Anthony Albanese argues that the law is needed to protect young people from the "harms" of social media, something many parent groups have echoed. A critical analysis of the ban reveals that it imposes excessive restrictions on social media usage, outweighing the benefits it aims to achieve. It is not the least restrictive step to protect children from cybercrimes. The government ignored the advantages which children acquire with the regulated usage of social media. A blanket ban is an extreme measure that curtails their right to information, expression, and social interaction. Instead of banning access, the government could have introduced stricter parental controls, mandatory safety settings, or digital literacy programs to educate children about raising awareness regarding threats on the internet and responsible online behaviour. *"The more sustainable approach is to guide teens on healthy online habits and responsible usage. Encouraging open discussions about risks and setting screen-time boundaries with parental support can be effective."(Says, Dr Kohli)* [18] The impact of this ban is also not very assessed on the psychological and social growth of the children in this modern society filled with social connection on fingers. The principle of "least restrictive means" suggests that regulation, rather than prohibition, would be a more balanced approach. Moreover, when they do gain access at 16, they may lack the necessary experience to navigate online spaces safely, making them even more vulnerable to cyber threats.

A fundamental flaw in the law is that it imposes the burden of protection of children on children themselves, by curtailing their freedom and access to social media, rather than addressing those responsible for cybercrimes. Instead of restricting children's access to social media, efforts should be directed at stopping cybercrimes, strengthening laws against online abuse, and ensuring accountability for platforms that fail to protect minors. Just as crimes in the physical world are addressed by punishing offenders, the digital space should be governed by similar principles. Restricting children from social media while allowing harmful content and bad actors to operate freely is an unfair and ineffective solution. While the intention behind the ban is understandable, its execution is flawed. Instead of banning social media, the government should have focused on digital education, parental controls, and stronger online safety measures. A well-regulated approach would have protected children without compromising their right to information, social development, and digital literacy. In the long run, policies that educate and empower children to use the internet safely will be far more effective than blanket bans.

3. Recommendations: For a Safer Online Space for Children

1) **Collaborative Participation from the Society:** A whole-of-society response is essential to tackle the factors that enable this serious child rights violation to proliferate.[19] Protecting children is a societal need, not just an effect of the bilateral relationship between child and parents. Because children are the future of society and going to contribute to the overall societal well-being. The challenge posed by the ever-evolving nature of cybercrime puts impetus on shareholders and requires active participation from them to prevent cybercrimes and suppress them.
2) **Enhanced Role of NGO:** Non-governmental organisations should be encouraged to be more active in this domain of child protection. NGOs play a crucial role

[14] Protection of Children from Sexual Offences Act 2012, s 13
[15] Yash Singh, 'Are Indian Cyber Laws Enough to Tackle Cybercrime' (2021) 27 Supremo Amicus [525]
[16] Tackling online violence against children, UNICEF. < https://tinyurl.com/y8jwm47t>
[17] Hannah Ritchie, Australia approves social media ban on under-16s, BBC News, Sydney. < https://www.bbc.com/news/articles/c89vjj0lxx9o> [Accessed on 5 feb, 2025]
[18] Bharati Mishra Nath, Analysis: Should India Ban Social Media For Under-16s, Like Australia?, NDTV, https://www.ndtv.com/india-news/analysis-should-india-ban-social-media-for-under-16s-like-australia-7019678 [Accessed on 6th Feb, 2025]
[19] Protecting children from sexual abuse and exploitation facilitated by digital technologies, UNICEF. < https://www.unicef.org/media/164421/file/Policy%20brief_Protecting%20children%20from%20violence%20in%20the%20digital%20environment.pdf.pdf> [Accessed on 5 feb, 2025]

in protecting children, especially in the digital age. They conduct surveys and collect data to study and understand the issue of online child abuse. NGOs also run awareness programs and workshops in schools and communities, filling a gap that the government often struggles to address. Since online child exploitation is a growing concern in India, research in this area is still limited. However, some NGOs have taken the initiative to study internet safety for children and continue to push for stronger protections and awareness. These NGOs and other government intermediaries should be entrusted with the responsibility of reporting any instances of cybercrime against children in the remote and backward regions of the country. Often, instances of cybercrimes committed on the population of these regions go unreported, making these backward regions an easy target for perpetrators of cybercrimes.

3) **Parent's Role:** Parents must engage with their children in their online activities, have knowledge of the online services used by them, help and assist the children in understanding and managing their personal information, and educate them on the dangers of meeting strangers etc.[20] Schools and teachers should educate students about cybersecurity, making sure they are aware of the risks and consequences of their digital actions. They must ensure that any learning software used in schools or coaching is safe, filtered, and regularly monitored. Additionally, if they come across any cybercrimes or online threats, they should take immediate steps to report them to the proper authorities.[21] Children should be encouraged to feel comfortable discussing their online experience with parents and teachers or anyone in whose custody they are. This will allow parents or other responsible members of society to immediately take action against any instance of cybercrime against the child to protect them.
4) **Government's Role:** Indian government leading the way in the right direction and contributing substantially with modern measures to protect children, departing away from blanket criminalisation. For instance, Under the Nirbhaya Fund, the government runs the Cyber Crime Prevention against Women and Children (CCPWC) project. This initiative focuses on raising awareness about cybercrimes, issuing alerts and advisories, training law enforcement, prosecutors, and judicial officers, and strengthening cyber forensic facilities to tackle online threats effectively.[22] A MoU is signed between the NCRB, India and the National Center for Missing and Exploited Children (NCMEC), USA regarding receiving of Tipline report on online child pornography and child sexual exploitation contents from NCMEC. The Tip lines, as received from NCMEC, are being shared with Stats/UTs online through the Nation Cybercrime Reporting Portal for further action.[23] MeitY through a program, namely, Information Security Education & Awareness (ISEA), has been creating awareness among users including women and children highlighting the importance of digital safety while using the Internet. A dedicated website for information security awareness (https://www.infosecawareness.in) provides relevant awareness material.[24] But there is still much to do by the government. The government should keep forming committees and panels and encourage debates in parliament regarding child safety and the internet. It is the responsibility of the government to enforce strict regulatory mechanisms to protect the interests of the children.
5) **Responsibilities of Tech-Industries:** The giant tech industries should also be imposed with the responsibility of protecting the children. The industries should use technological expertise to develop procedures and features that identify and mitigate content risks early on and remedy their impact on children. Greater investment in content moderation is needed. Child-friendly mechanisms for reporting hate messages and violent images online should be developed and supplemented by educational materials to raise children's awareness about these problems and how to report them. There should be clear and child-friendly terms of service and codes of conduct that discourage the creation and distribution of hateful and violent content, and companies should be encouraged to restrict access to these services for repeat offenders.[25]
6) **International Solidarity:** This is not just a challenge for individual countries to address to protect their people. It goes beyond a simple exchange between states and their citizens, carrying broader implications that affect societies on a larger scale. Therefore, There is an urgent need for countries should coordinate at the global level to tackle this transnational problem. As cyberthreat and child protection are not a regional concern or restricted to the territory of a country. UNICEF, the Human Rights Commission and the United Nations are calling for a coordinated approach from governments all around the globe. Most countries have noticed cyberbullying as a crime and made an effort to prevent cyberbullying.[26] While it is not possible to completely reduce the risk of children being exposed to potentially harmful content online, countries that have managed to curb exposure can serve as good examples both to countries currently facing greater risk and to those transitioning from low to high connectivity.[27]

---

[20] Dr. Nagarathna A., Jay Bhaskar Sharma, Sparsh Sharma. 'Children and Child Safety-an-e-book. Advance Centre for Research, Development and Training in Cyber Laws and Forensics,' National law school of India university Bangalore. (p. 4)
[21] Ibid.
[22] Online Cyber Grooming of Women and Young Children, Press Information Bureau, Ministry of Women and Child Development of Government of India. < https://pib.gov.in/Pressreleaseshare.aspx?PRID=1806602> [Accessed on 5 feb, 2025]
[23] Ibid.
[24] Ibid.
[25] [25] Daniel Kardefelt Winthera , Mariya Stoilovab , Moritz Büchia , Rogers Twesigyea , David Smahelc , Marie Bedrosovác , Nikol Kvardovác , Sonia Livingstoneb, Children's exposure to hate messages and violent images online, UNICEF. https://www.unicef.org/innocenti/media/2621/file/UNICEF-Children-Exposure-Hate-Violence-Online.pdf
[26] Baldry, A., Blaya, C. and Farrington, D., 2018. *International perspectives on cyberbullying*. Palgrave studies in cybercrime and cybersecurity. London: Palgrave MacMillan.
[27] Daniel Kardefelt Winthera , Mariya Stoilovab , Moritz Büchia , Rogers Twesigyea , David Smahelc , Marie Bedrosovác , Nikol Kvardovác , Sonia Livingstoneb, Children's exposure to hate

7) **Role of Educational Institutions:** Cyber safety should be introduced as a mandatory subject in school curriculums, ensuring that children understand online risks such as cyberbullying, phishing, identity theft, and exploitation. Teaching students about responsible internet usage, privacy protection, and safe online interactions will help them navigate the digital world confidently and securely. Teachers and school staff must be trained to recognize signs of online abuse, such as sudden behavioural changes, withdrawal from social interactions, or distress linked to internet use. Organizing regular workshops for educators will help them identify potential cases of cyber harassment and take timely action to support affected students. Schools should also collaborate with parents, law enforcement agencies, and cybersecurity experts to create a safer online environment for children. By integrating digital literacy and safety into education, we can empower children to use technology responsibly while minimizing their exposure to cyber threats.

4. Conclusion

The internet has become an important part of children's lives, offering both opportunities and risks inherent with it. While the digital space enables children to learn, communicate, and explore the modern digital world, it also exposes them to dangers such as cyberbullying, online exploitation, and data privacy threats. Indian laws, including the IT Act, IPC, and POCSO Act, provide some protection, but they are not fully equipped to handle the evolving nature of cybercrimes against children. The rapid advancement of technology has created new challenges that existing laws fail to address effectively. To ensure a child's safety online, a collective effort is needed from the society. Parents must actively monitor and guide their children's internet use, schools should educate students about cybersecurity. The government must update and strengthen laws to keep pace with digital threats. Roles of The NGOs should be recognised, as they also play a crucial role in spreading awareness in backward areas and conducting research on child protection in cyberspace. While initiatives like the Nirbhaya Fund and CCPWC are steps in the right direction, more needs to be done to create a safer online environment for children. By improving legal frameworks, increasing awareness, and encouraging responsible digital behaviour, India can ensure that children benefit from the internet while staying protected from its dangers.

messages and violent images online, UNICEF. https://www.unicef.org/innocenti/media/2621/file/UNICEF-Children-Exposure-Hate-Violence-Online.pdf