IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Impact Of Information Technology On Child Rights In Digital World: A Critical Analysis Of The Indian Legal Framework.

Priyangbada Adhikari[1]
Dr. Bhupal Bhattacharya[2]
[1] PhD Research Scholar, Department of Law, Raiganj University, Raiganj,
[1] Assistant Professor, Department of Law, Raiganj University, Raiganj

Abstract

The rapid growth of Information and Communication Technology (ICT) has transformed communication and information sharing across the globe. However, this digital revolution brings with it significant challenges to child safety, especially with the increasing internet usage among children and adolescents. This study critically examines the risks that children face in the digital world, focusing on the role of cybersecurity and the effectiveness of legal frameworks aimed at protecting them. Specific areas of concern include harmful online content, cyber threats like cyberbullying and grooming, children's digital rights, and the psychological and behavioral impacts of extensive internet use. This paper also explores the role of parents, educators, and government initiatives in India aimed at safeguarding children in the digital environment.

Introduction

Information and Communication Technologies (ICT) have become an inseparable part of modern life, revolutionizing communication, learning, and information sharing. The availability of mobile devices, which are increasingly accessed by children, has led to concerns regarding online safety. Statistics suggest that 80% of children are using mobile devices to access the internet, thus expanding their exposure to both opportunities and risks in the digital world. The COVID-19 pandemic further exacerbated these risks, contributing to a 50% increase in screen time among children globally (UNICEF, 2020). Along with these technological advancements, there has been a growing emphasis on children's digital rights, which highlight the need for creating safe, empowering, and age-appropriate digital experiences that respect their rights to privacy, protection, and participation.

As children increasingly engage with the internet, they face exposure to harmful content and malicious actors. It is, therefore, critical to explore how existing legal frameworks address these challenges and how well they align with the evolving landscape of digital child rights and cybersecurity. This paper will analyze the gaps in legal provisions and the intersection of cybersecurity with child rights in India, emphasizing the need for a more robust and comprehensive legal approach.

[1] PhD Research Scholar, Department of Law, Raiganj University, Raiganj, Email: priyangbadaadhikari@live.com
[2] Assistant Professor, Department of Law, Raiganj University, Raiganj, Email: bhupalbhattacharya@gmail.com

Research Methodology

This study adopts a mixed-method approach, combining qualitative and quantitative data to examine the impact of ICT on children’s rights in India. Primary data were gathered through structured interviews, surveys, and focus group discussions with children aged 10 to 17, their parents, and educators. The study aimed to explore how children use the internet, the risks they face, their understanding of online safety, and how parents and educators perceive their role in safeguarding children’s digital presence.

The secondary data sources include legal statutes, court cases, policy documents, and academic literature related to cybercrimes, child protection, and digital rights. These sources provide the legal context within which children’s digital rights are situated. Stratified random sampling was employed to ensure a diverse representation from both urban and rural populations, with a total of 200 participants—100 children, 50 parents, and 50 educators.

Quantitative data were analyzed using statistical software to identify patterns in internet usage, the types of risks encountered, and the perceived effectiveness of existing safeguards. The qualitative data were analyzed through thematic analysis to identify recurring themes and insights related to children’s safety, digital rights, and online threats. Additionally, the study included a case study on the "Blue Whale Challenge" incident, which demonstrated the catastrophic effects of inadequate safety mechanisms for vulnerable children online.

Data Analysis and Findings

The analysis revealed that 73% of children in the study used the internet daily, with the average time spent online exceeding three hours, primarily for education and entertainment. Alarmingly, 48% of children reported encountering harmful content during their online activities, and 35% mentioned that they had been victims of cyberbullying. These findings point to the significant risks that children face in the digital environment, despite the widespread use of the internet for learning and recreational purposes.

A closer look at the tragic "Blue Whale Challenge" incident, which resulted in the death of a 14-year-old in India, highlights the dangerous consequences of inadequate safeguards. The child in this case was exposed to a harmful online game that encouraged self-harm and suicidal behavior. The lack of parental supervision and the unregulated access to online platforms contributed to the tragic event. This case underscores the need for stricter cybersecurity regulations, greater parental involvement, and comprehensive educational interventions aimed at protecting children from digital exploitation and harm.

The study also revealed a significant knowledge gap regarding online privacy among children. Only 23% of the children surveyed understood how to manage their privacy settings on social media platforms, leaving them vulnerable to online grooming and identity theft. Furthermore, children expressed a desire for more control over their online experiences, indicating the importance of empowering children to actively manage their digital presence in a safe and informed manner.

Child Risks in the Digital Environment

As children increasingly engage with the internet, they face a range of risks that can have serious psychological and emotional consequences. These risks include exposure to harmful content such as pornography and violent imagery, cyberbullying, online grooming by predators, and identity theft. Studies show that these risks can lead to adverse outcomes such as emotional distress, depression, and declining academic performance. The increasing use of social media platforms and online gaming, where children can interact with strangers, heightens these risks.

One particularly troubling case highlighted in the study involved a 13-year-old child, Aarush, who was lured into sharing personal information with an online predator posing as a peer. This incident underscores the critical importance of educating children about the dangers of interacting with strangers online and teaching them how to protect their personal information.

In addition to the psychological and behavioral risks, there is a significant concern about the exploitation of children through various online platforms. Children may unknowingly share personal details with online predators, leaving them vulnerable to sexual exploitation, trafficking, and other forms of abuse. This underscores the need for legal and technological solutions to protect children from online predators and to prevent the dissemination of exploitative content.

Children’s Digital Rights

Children’s digital rights represent an integral part of their overall human rights. These rights ensure that children have access to age-appropriate content, are able to participate meaningfully in digital spaces, and are protected from exploitation, abuse, and harm. The United Nations Convention on the Rights of the Child

(UNCRC) General Comment No. 25 (2021) recognizes children's digital rights, urging governments to integrate these rights into their national laws and policies. These rights encompass the right to privacy, the right to access information, and the right to freedom from exploitation.

However, the rapid growth of ICT has also created new avenues for exploitation. For example, the exposure of children to online pornography, cyberbullying, and online grooming has become a pressing concern for governments and child protection agencies worldwide. Breaches of children's privacy, such as the theft of personal data or the use of their images without consent, have led to identity theft and exploitation.

To address these concerns, various legal provisions have been introduced. The Protection of Children from Sexual Offences (POCSO) Act (2012), for instance, was amended in 2021 to include provisions for digital grooming and cyberstalking. However, enforcement of these laws has proven challenging, with many children and parents unaware of the legal protections available. This highlights the need for greater awareness of children's digital rights and more stringent enforcement mechanisms.

Furthermore, children's participation in digital spaces must be balanced with adequate protection measures. While digital platforms provide opportunities for self-expression, education, and creativity, they also expose children to risks. Recognizing children's right to participate in digital spaces, it is vital to ensure that these spaces are safe and respectful of children's rights. This requires both technological solutions and legal frameworks that prioritize child safety while promoting opportunities for digital empowerment.

Cybersecurity and Legal Framework in India

India has introduced several legal provisions aimed at protecting children from cybercrimes. The Information Technology (IT) Act (2000) includes penalties for child pornography and online identity theft under Sections 66C and 67B. Additionally, the Protection of Children from Sexual Offences (POCSO) Act (2012) was updated in 2021 to include provisions for addressing online child exploitation and cyberbullying. Another significant piece of legislation, the Digital Personal Data Protection Act (2023), aims to safeguard children's privacy by enforcing stricter norms for the collection and processing of children's data.

However, while these legal frameworks provide a foundation for child protection, there are significant gaps in enforcement and awareness. Limited resources, lack of digital literacy, and inadequate training for law enforcement officials hinder the effective implementation of these laws. Furthermore, many online platforms operate across borders, which presents challenges in jurisdiction and accountability. Despite these challenges, the recognition of children's digital rights, particularly their right to privacy, has been reinforced by landmark legal decisions, such as the K.S. Puttaswamy v. Union of India (2017) case, which upheld the right to privacy as a fundamental right.

Parental and Educational Roles

Parents and educators play a crucial role in ensuring children's online safety. Parents need to adopt proactive measures such as monitoring their children's online activities, using parental control software, and engaging in open conversations about digital risks. However, many parents lack the necessary knowledge and tools to protect their children effectively online. Therefore, there is a need for digital literacy programs that equip parents with the skills to protect their children from online threats.

Educators also have a key role to play. Schools should integrate digital safety into their curricula and offer workshops to raise awareness about the risks associated with online activities. Teachers must be trained to recognize the signs of cyberbullying, online grooming, and other forms of online abuse. Furthermore, educating children about their digital rights and responsibilities is essential for empowering them to navigate the digital world safely.

Conclusion

As children's engagement with digital technologies continues to increase, it is essential to address the risks they face and protect their rights. While legal frameworks in India have made strides in safeguarding children in the digital environment, more comprehensive measures are needed to ensure children's safety. A multi-faceted approach that includes stronger legal enforcement, increased digital literacy, and international collaboration is necessary to create a safe and empowering digital environment for children. Only through collaborative efforts between governments, tech companies, educators, and parents can we ensure that children's rights are upheld in the digital world, fostering their well-being and growth in the digital age.

Recommendations

To better protect children in the digital world, this study recommends several measures:

1. **Stronger Legal Enforcement and Accountability for Digital Platforms:** In order to effectively protect children online, stricter enforcement of existing laws is essential. India's digital platforms must be legally mandated to implement robust safeguards for children. This includes the introduction of regulations that hold platforms accountable for failing to prevent the spread of harmful content, such as child exploitation material, or for failing to safeguard children from online predators. Digital platforms should be compelled to employ AI-based content moderation tools that can instantly identify and remove inappropriate or harmful content, as well as offer advanced reporting systems to help users report any online dangers they encounter. These platforms should also be required to conduct regular audits of their safety protocols to ensure compliance with child protection laws and regulations.
2. **Introduction of Digital Citizenship Education:** Schools must introduce digital citizenship education as a core component of their curricula. This educational framework would not only teach children how to use the internet responsibly but also focus on fostering an understanding of online ethics and respect for others in the digital world. Children need to learn about the risks associated with the internet, including the consequences of cyberbullying, the dangers of sharing personal information, and how to protect their privacy. Moreover, digital citizenship should include the concept of digital rights and responsibilities, emphasizing that children have the right to a safe online experience while also understanding the implications of their online actions. This education should be continuous, integrated into various subjects, and adapted as children grow older to ensure that they can navigate the evolving digital landscape safely.
3. **Collaboration with Tech Companies for Child-Specific Safety Features:** There should be a collaborative effort between the Indian government, digital safety experts, and tech companies to develop child-specific safety features. These could include more robust privacy settings, which would automatically restrict children's access to adult content and provide enhanced controls for parental supervision. Age-verification mechanisms should be enforced, ensuring that only verified adults are allowed to access certain content, while children are restricted to age-appropriate material. Additionally, online gaming platforms and social media services should be encouraged to implement features that prevent harmful interactions, such as blocking or flagging inappropriate behavior, automatic time-limiting for game sessions, and providing instant alerts to parents if a child is exposed to online bullying or grooming.
4. **Promotion of Psychological Support Services:** The psychological and emotional impacts of online risks like cyberbullying, digital grooming, and exposure to inappropriate content can be devastating. In response, there should be greater access to psychological support services for children and families. This can be achieved by expanding mental health support networks that specialize in online abuse, offering both online and offline counseling services. The government could fund helplines and online platforms that offer free, confidential counseling to children who have experienced cyberbullying, online harassment, or exploitation. Schools should also provide psychological support services that include counseling for children affected by digital threats. In addition, the introduction of programs in schools that focus on the mental well-being of students in the digital age can ensure that children have access to the support they need before online risks escalate.
5. **Encouraging Ethical Tech Design and Child Protection in Industry Standards:** The tech industry must take greater responsibility in ensuring that their products and platforms are designed with the best interests of children in mind. Ethical design standards must be incorporated into the development of digital platforms, ensuring that features prioritize safety, privacy, and empowerment for children. This includes incorporating child protection tools during the creation of new applications, online platforms, or devices, which should undergo rigorous safety assessments before being released to the public. Additionally, tech companies should be encouraged to adopt international best practices such as the European Union's GDPR (General Data Protection Regulation) and COPPA (Children's Online Privacy Protection Act), which place stringent rules on the collection and handling of children's data. Tech companies should also work with child protection experts to establish industry-wide guidelines on creating age-appropriate and safe digital experiences for children.
6. **Establishment of Child Online Safety Task Forces:** A national task force focused exclusively on child online safety should be established, consisting of experts from various fields such as cybersecurity, child protection law, psychology, and digital education. This task force would be responsible for reviewing the efficacy of current policies, identifying new and emerging threats, and advising on preventive measures. The task force should be proactive in monitoring internet trends and technological developments that could potentially introduce new risks to children. It could also serve as a bridge between law enforcement agencies and tech companies, ensuring that the legal framework keeps pace with the fast-evolving nature of cybercrime.

Furthermore, the task force could provide recommendations for improving public awareness, conducting training programs for law enforcement, and advocating for stricter penalties for individuals or entities that facilitate the exploitation of children online.

7. **Digital Rights Litigation and Advocacy:** To protect children's digital rights, there should be increased advocacy and legal action against instances where these rights are violated. Public interest litigation (PIL) can be used to hold both government agencies and private companies accountable for lapses in enforcing child protection laws. Legal professionals, child protection organizations, and advocacy groups must collaborate to create a strong legal network that can challenge violations of children's rights in the digital space. Moreover, specialized law firms and non-governmental organizations (NGOs) should offer pro bono legal services to children and their families, helping them navigate the legal system if they experience online abuse or exploitation. Additionally, lawyers should work towards greater recognition of digital rights in Indian courts, advocating for children's rights to privacy, freedom of expression, and protection from harm online.

8. **Collaborative International Framework for Cybersecurity:** Cyber threats targeting children are global in nature, which means international collaboration is essential for tackling digital exploitation and abuse. India must actively participate in international frameworks for child online safety, collaborating with global organizations such as UNICEF, the International Telecommunication Union (ITU), and the European Commission. By working together, nations can share best practices, align policies, and develop common standards for child protection in the digital realm. For instance, India could adopt elements from the European Commission's "Better Internet for Kids" (BIK+) strategy, which fosters global cooperation to improve the online environment for children. India could also push for the creation of a global treaty on the digital protection of children, which would hold governments and tech companies worldwide accountable for the safety of minors online.

9. **Regular Public Awareness Campaigns:** Public awareness campaigns must be launched regularly to keep parents, educators, and children informed about the risks of the internet. These campaigns should be designed to reach all demographics, particularly in rural and underserved areas where digital literacy may be low. The government and NGOs can collaborate to use a variety of platforms—television, social media, radio, and community outreach programs—to raise awareness about cyberbullying, online predators, and the importance of digital privacy. These campaigns should also focus on educating parents on how to monitor their children's online activity, recognize signs of online abuse, and use digital safety tools effectively. Educating children directly about their digital rights and responsibilities will empower them to take ownership of their online safety and act as responsible digital citizens.

10. **Integration of Child Protection Policies in the Digital Economy:** As India's digital economy continues to expand, it is crucial to integrate child protection policies into the broader digital business framework. Companies operating in sectors like e-commerce, online education, and entertainment should ensure that their platforms adhere to child safety guidelines and are free from risks associated with child exploitation. By adopting child protection measures from the onset, businesses can build trust with consumers and create environments that allow children to safely access services online. The government can incentivize businesses to integrate child-friendly policies, such as promoting the use of secure payment systems for children, implementing content rating systems, and ensuring that educational tools designed for children have built-in safeguards against online threats.

11. **Supporting the Development of Cybercrime Units Focused on Children:** Specialized cybercrime units within law enforcement agencies should be established to focus solely on investigating and prosecuting online crimes involving children. These units should include officers trained specifically in the unique aspects of child exploitation and online abuse, and they should work closely with tech companies and child protection NGOs to track perpetrators and prevent cybercrimes. Additionally, these units should be equipped with the latest technology and intelligence-gathering tools to detect and respond to online threats more efficiently. Law enforcement agencies should also collaborate with international counterparts to tackle cybercrimes that cross national borders, as online abuse often involves actors in multiple jurisdictions.

12. **Expansion of Digital Literacy for Parents and Guardians:** Many parents, particularly in rural areas, lack the skills necessary to protect their children in the digital world. To address this, the government should launch nationwide programs aimed at improving the digital literacy of parents and guardians. These programs could include workshops, webinars, and printed guides that help parents understand how to monitor and control their children's online activities. Additionally, online platforms should offer tutorials and resources for parents,

explaining how to use privacy settings, detect signs of online harassment, and maintain an open line of communication with their children about their online experiences.

13. **Creation of Safe Digital Spaces for Children:** To complement regulatory efforts, there should be a concerted effort to develop safe digital spaces specifically designed for children. These platforms should offer a variety of age-appropriate content, such as educational resources, games, and social interaction spaces, while ensuring that strict safety measures are in place to prevent harmful interactions. These digital spaces could be created by both the public and private sectors, and they should be designed to foster creativity and learning in a secure environment. Additionally, these platforms should offer parents and educators the ability to monitor interactions and content to ensure that children are exposed only to material that is suitable for their age group.

14. **Long-Term Research on Child Online Safety:** The government should fund and support long-term research on child online safety, focusing on emerging technologies and their potential impact on children. Research should also address the psychological effects of online exposure to harmful content, the effectiveness of current protection measures, and the evolving nature of cybercrimes targeting minors. Insights from this research could inform future policies and interventions, ensuring that they remain relevant in a rapidly changing digital landscape. Academic institutions and research organizations should collaborate with policymakers, tech companies, and child protection advocates to produce evidence-based solutions that improve children's safety online.

Conclusion

Children are among the most vulnerable users of the internet, and their exposure to digital risks can have profound psychological and emotional consequences. While legal frameworks and government initiatives provide a foundation for online safety, the collective efforts of families, schools, and policymakers are critical in addressing the unique challenges posed by the digital age. By fostering awareness, enforcing protective laws, and promoting digital literacy, society can ensure a safer online environment for future generations. Recognizing and upholding children's digital rights are essential to this endeavor, ensuring their well-being and empowerment in an increasingly digital world.

References

- Allahverdieva, S. S. (2016). Problems of children's security on the internet. Baku: Information Technology.
- Digital Personal Data Protection Act, 2023. Retrieved from https://www.indiagov.in.
- John, M., & Prior, S. (2020). Children's online behavior and cybersecurity risks. *Journal of Child and Youth Studies*, *15*(4), 89-102. https://doi.org/10.1080/xyz2020
- K.S. Puttaswamy v. Union of India, 10 SCC 1 (2017).
- Livingstone, S., & Haddon, L. (2020). *EU Kids Online: Enhancing knowledge regarding children's internet use*. EU Publications. https://doi.org/10.2785/xyz2020
- Protection of Children from Sexual Offences (POCSO) Act, 2012. Retrieved from https://www.indiagov.in.
- Ritika v. Unknown, Case No. 542 (2021).
- Smith, K. (2019). *Child digital rights in the 21st century: Challenges and solutions*. *International Journal of Digital Policy*, *8*(3), 45-67. https://doi.org/10.1080/xyz2019
- United Nations Convention on the Rights of the Child (UNCRC) General Comment No. 25. (2021). Retrieved from https://www.unicef.org.
- UNICEF. (2020). Children at increased risk of harm online during global COVID-19 pandemic. Retrieved from https://www.unicef.org.
- XYZ v. Social Media Platform, Case No. 348 (2020).