IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

"An Analytical Study on Child Cyber abuse and Laws Relating to Protection of Child from Cyber abuse in Gujarat"

Niddhi Dinesh Bhai Gohil

Research Scholar, GLS University Ahmedabad.

Dr. Vaishakhi Thaker

Assistant Professor Faculty of Law , GLS University Ahmedabad.

Abstract:

This research aims to provide a comprehensive analysis of child cyber abuse and the legal framework for child protection against cyber abuse in the state of Gujarat, India. The study employs methods qualitative analyses. qualitative data is collected through interviews with legal experts, child psychologists, and law enforcement officials to gain deeper insights into the dynamics of cyber abuse cases and the efficacy of existing legal measures. Key findings reveal a concerning prevalence of cyber abuse incidents targeting children in Gujarat. These abuses range from cyberbullying, online harassment, grooming, to exposure to inappropriate content. The research identifies the internet's anonymity and accessibility as key factors contributing to the vulnerability of children to such abuses. Furthermore, the study provides a detailed examination of the legal framework in [1]Gujarat concerning child protection from cyber abuse. It critically evaluates the effectiveness of current laws, such as the Information Technology Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, in addressing the challenges posed by evolving cyber threats. The research identifies gaps in these laws, particularly in terms of enforcement, awareness, and integration with digital platforms. In conclusion, this study underscores the urgent need for a holistic approach to combat child cyber abuse in Gujarat. It advocates for enhanced legal measures, educational campaigns, and collaborative efforts among stakeholders, including parents, schools, law enforcement, and tech companies. By bridging these gaps, Gujarat can create a safer digital environment for its children, ensuring their well-being and protection in the ever-evolving [2]digital landscape.

[1] A Historical Perspective. International Journal of Criminology and Sociology, 7, 121-134.

[2] Barua, A. (2018). Child Protection in India:

Keywords: Child cyber abuse, Online exploitation, Cyberbullying, POCSO Act, Law enforcement.

1 INTRODUCTION:

In the digital era, children face escalating risks of cyber abuse, necessitating a thorough examination of these challenges. This study delves into the landscape of child cyber abuse within Gujarat, India, scrutinizing its diverse manifestations and consequences. By assessing the effectiveness of existing legal safeguards, policies, and their enforcement, the research aims to identify gaps and propose enhancements. Through this inquiry, it seeks to elevate awareness of this pressing issue, providing insights to fortify protections for children in Gujarat's ever-evolving digital milieu, ultimately striving for a safer online environment for the state's young population.

- **Child:**

According to The Protection of Children from Sexual Offenses Act,2012'[3]s Section 2(d), "child" refers to anyone under the age of 18

The Juvenile Justice (Care and Protection of Children) Act, 2015 defines a child as "a person who has not attained the age of eighteen."

The Prohibitions of Child Marriage Act of 2006 defines a child as a person who, if a male, has not reached the age of twenty-one and, if a female, has not reached the age of eighteen.

According to The Protection of Children from Sexual Offenses Act, 2012's Section 2(d), "child" refers to anyone under the age of 18

- **Child Abuse:**

Child abuse or maltreatment, in the words of the World Health Organization, "constitutes all forms of physical and/or emotional ill-treatment, sexual abuse, neglect or negligent treatment, or commercial or other exploitation, resulting in actual or potential harm to the child's health, survival, development, or dignity in the context of a relationship of responsibility, trust, or power".

- **Child Cyber Abuse:**

The term "child cyber abuse" has no specific definition. Any abuse that takes place online qualifies. Any web-connected device, including PCs, tablets, and mobile phones, is susceptible to it. Additionally, it can occur anywhere on the internet, including on social media, in text messages and messaging applications, emails, online chats, online gaming, and live streaming websites. Several laws exist in India to protect children from online abuse, but regrettably some offences, such as child cyberbullying, have not been specifically addressed. Even the age defined in the amended Act of 2008 raises questions because, despite the social networking sites' rules and age restrictions while using them, there is no perfect way to determine a user's age. Even the definition of the word "kid" varies depending on the context. There are certain gaps in the law, thus comprehensive legislation is needed to protect youngsters.

[3] The Protection of Children from Sexual Offences Act, 2012.

1.1 Research Problem:

The prevalence and severity of child cyber abuse in Gujarat[4], India, pose significant challenges to the safety and well-being of minors in the digital age. Despite existing legal frameworks and initiatives aimed at addressing these issues, gaps persist in effectively combating this complex phenomenon. Key problems include the underreporting of cyber abuse incidents, inadequate awareness among parents and caregivers about online risks, evolving tactics used by perpetrators to exploit children online, and the need for continuous adaptation of legal frameworks to keep pace with emerging threats. Additionally, the lack of comprehensive data on the nature and extent of child cyber abuse in Gujarat hampers informed decision-making and targeted interventions. Addressing these challenges requires a nuanced understanding of the multifaceted dimensions of child cyber abuse within the state, as well as actionable recommendations to enhance legal protections, awareness programs, and enforcement mechanisms. This research seeks to delve into these pressing issues, aiming to illuminate the path toward a safer digital environment for Gujarat's children.

1.2 Research Objectives:

1. To analyze the prevalence and forms of child cyber abuse within the digital landscape of Gujarat, India.
2. To assess the effectiveness and adequacy of existing legal frameworks, policies, and institutional mechanisms in safeguarding children from online threats.
3. To identify gaps and challenges in the implementation of laws related to child cyber abuse in Gujarat.

1.3 Research Hypothesis:

1. The incidence of child[5] cyber abuse in Gujarat, India, is expected to be significant, encompassing various forms such as online harassment, cyberbullying, grooming, and exploitation.
2. It is hypothesized that there will be identifiable gaps in the enforcement and implementation of existing legal frameworks, necessitating targeted interventions to enhance the protection of children from cyber abuse in the state.

1.4 Scope of Research:

This research focuses on the landscape of child cyber abuse within the specific context of Gujarat, India, examining prevalent forms such as online harassment, cyberbullying, grooming, and exploitation. The study will analyze the adequacy and effectiveness of existing legal frameworks, including the Information Technology Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, in addressing these issues. Additionally, it will explore challenges in the implementation of laws related to child cyber abuse and propose recommendations for policymakers, law enforcement agencies, educators, and stakeholders to enhance protections and promote awareness in the state.

[4] Retrieved from https://wcd.nic.in/act/pc-so-act-2012

[5] Chawla, A., & Garg, A. (2017). Cyber safety for children: A study of awareness levels among parents and guardians in India. International Journal of Engineering and Computer Science, 6(6), 21907-21912.

1.5 Research Questions:

1. What are the prevalent forms of child cyber abuse experienced by minors in Gujarat, India?
2. How effective are the existing legal frameworks and policies in Gujarat in protecting children from online threats and exploitation?
3. What are the key challenges and gaps in the implementation of laws related to child cyber abuse within the state?

   What actionable measures can be recommended to enhance awareness and bolster protections for children against cyber abuse in Gujarat?

1.6 LITERATURE REVIEW:

1.6.1 Cyber Law Indian & International Perspective By Aparna Viswanathan:

This book addresses a wide range of cyber law-related themes, including cloud computing, obscenity and child pornography, intermediary responsibility, data security, and other significant concerns from both Indian and international perspectives. The privacy right the subject that attracted the most interest in the context of cyberspace

Research Gap: The author of this book addressed the right to privacy in the context of cyber space; however, they did not address the invasion of children's private or their human rights.

1.6.2 Protection of Children on Internet By Karnika Seth:

The book's main focus was on how children use the Internet, a topic that concerns parents, teachers, law enforcement, and internet service providers, among other stakeholders.

Research Gap: The author of this book expressed concern about the harmful effects of the internet on children, but she did not suggest any preventative actions.

1.6.3. A Practical approach to Cyber Laws - by Mani:

This book examined the steps taken by the Indian legal system to protect citizens' internet privacy. It covered a lot of ground in terms of the various kinds of cybercrimes, the acceptance of digital evidence, and how judges perceive cyberspace incidents. This book is a helpful resource for several case studies of cybercrimes in India. It also addressed the entirety of the Information Technology Act of 2000's rules, specifications, and other obligations.

Research Gap: Though it is silent on children's online safety, this book offers helpful information about the laws that are in place to deal with cybercrimes in cyberspace and acknowledges the use of digital evidence in such cases.

1.6.4. Network Security : A Hacker's Perspective By Ankit Fadia:

This book is an excellent source of information about cybercrime tactics and countermeasures. Learning about network security should be everyone's top priority. This book examined a variety of network security issues and provided the best methods for protecting them.

Research Gap: Despite providing an excellent guide on how to combat such crimes and deftly describing the tactics used by criminals, the author of this book regretfully demonstrated little concern for the invasion of children's online rights.

1.6.5. Haresh A. Shukla's Criminal Court Handbook, sixth edition 2013,

Kamala Publication House, Rajasthan as the publisher Each of the three principal acts—the Indian Penal Code of 1860, the Code of Criminal Procedure of 1973, and the Indian Evidence Act of 1872, updated with commentary and revisions.

Research gap: This book mostly discusses the laws now in place to combat cybercrimes, but it makes no mention of the necessity of passing laws to shield minors from abuse they may face online.

1.6.6. Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions:

The topic of cyberbullying in Indian universities is discussed: Except for a tiny percentage of respondents who don't have access to the internet or personal devices, this case study showed that 97% of respondents in Institutions of higher learning possess electronic equipment. Even in the UNICEF case study, it was demonstrated that 99 percent of internet users in both urban and rural areas who were 12 years of age or older utilized mobile phones. The most widely used social media sites, Instagram and WhatsApp, increase their vulnerability to cyberbullying. The comments made by the participants indicate that they are not well-versed in the definition of "cyberbullying," the associated legal limits, or other anti-government policies.

Research gap: This case study focused on the term "cyberbullying" and looked at how much youngsters currently know about their online rights, however it was not very thorough. limiting the analysis to a single offense, creating a gap.

1.6.7. Cyber Laws By Dr. Gupta & Agrawal:

This book is a must-read for anyone just starting off. After going over the fundamentals of computers, it covered subjects including encryption technology, the contractual and evidentiary aspects of cyber laws, intellectual Digital-age property rights, online consumer protection, etc. It was mostly focused on cybercrimes and the shortcomings of the 2000 Indian Information Technology Act.

Research gap: The book's author concentrated on legal pitfalls, the evidence-based character of cyber laws, and internet concepts; nevertheless, she did not address the systemic changes that are required.

1.7 Research Methodology:

This study employs a mixed-methods approach to comprehensively investigate child cyber abuse in Gujarat, India. Quantitative methods involve the collection and analysis of data from surveys or questionnaires distributed among parents, caregivers, educators,[6] and children themselves. This data will provide insights into the prevalence, forms, and impacts of cyber abuse. Qualitative methods, such as interviews and focus group discussions with key stakeholders including law enforcement officials, legal experts, and child welfare advocates, will offer deeper understanding of implementation challenges, gaps in protections, and recommendations for improvement. Additionally, a thorough review of existing literature, laws, and policies related to child cyber abuse in Gujarat will provide a foundational understanding for the analysis. This mixed-methods approach aims to offer a comprehensive view of the issue, combining quantitative data for statistical

[6] Childline India Foundation. (n.d.). About Childline. Retrieved from https://www.childlineindia.org.in/about-childline.htm

analysis with qualitative insights for a nuanced understanding of the landscape of child cyber abuse in Gujarat, India.

2. Types and Impacts of Child Cyber Abuse in Gujarat:

This section will provide an in-depth analysis of the various types of cyber abuse faced by children in Gujarat. It will explore real-life case studies and examples to illustrate the prevalence and severity of cyberbullying, online harassment, cyberstalking, and exposure to harmful online content. Furthermore, the section will delve into the detrimental effects of cyber abuse on children's self-esteem, mental health, academic performance, and social relationships.

2.1 Legal Framework for Child Protection in Gujarat: A critical aspect of this research is the examination of the legal provisions and mechanisms in place to safeguard children from cyber abuse in Gujarat. This section will analyze relevant national and state laws, including the Information Technology Act, 2000, and the Juvenile Justice (Care and Protection of Children) Act, 2015, along with any specific laws or policies pertaining to child protection in the digital realm.

2.2 Challenges and Gaps in the Legal System: Despite the existence of laws aimed at protecting[7] children from cyber abuse, this section will highlight the challenges and gaps in the current legal framework. Issues such as jurisdictional complexities, difficulties in evidence collection, and the need for enhanced coordination between law enforcement agencies and digital platforms will be discussed. Additionally, the section will address the challenges faced by educators and parents in educating children about online safety and responding to incidents of cyber abuse.

2.3 Recommendations and Best Practices: Drawing from the analysis of existing literature and the legal framework, this section will propose recommendations for improving child protection from cyber abuse in Gujarat. Suggestions may include amendments to existing laws, establishment of specialized cybercrime units, enhanced digital literacy programs in schools, and collaboration between stakeholders such as law enforcement agencies, schools, parents, and internet service providers.

3. Comprehensive legislation in India is required due to the following reasons:

The increasing issue of child online abuse in India is not sufficiently addressed by the laws already in place. If children's safety [8]regulations are disregarded, social media platforms and online services Suppliers should be subject to strict liability.

In order to prosecute offenders outside of the court system, the term "kid" needs to be defined uniformly. To address particular offenses like cyberbullying, separate laws are required.

[7] Sharma, S., & Pandit, M. (2021). Child Online Protection: Issues and Challenges. International Journal of Human Rights in Healthcare, 14(3), 258-271.

[8] State Commission for Protection of Child Rights. (2018). Annual Report on Child Cyber Abuse cases in Gujarat.

3.1 Legal Framework to deal with cybercrimes in India:

Information Technology Act, 2000 (such Act)

(A) Section 66B: This section confirms a possible illegal acquisition of computer or communication equipment and sets down the penalty for receiving such.

three years behind bars. The severity of the offence may also result in a sentence of up to Rs. 1lakh. The main topics covered by Section 66C are password hacking, digital signatures, and other identity theft techniques. This section carries a maximum sentence of three years in prison as well as a fine of one lakh rupees.

(B) part 66D: This part deals with using computer resources to cheat by pretending to be someone else. If found guilty, the highest penalty is one lakh rupees and the maximum term is three years in prison. Publicating or transmitting images of personala Section 66E is violated when locations are used without the owner's permission.

(C) Section 67 B: This is a crucial legal provision that provides protection for actions taken online. Online offenses against minors are recognized under this statute.

The following offenses are included in the statute as crimes against minors. objectionable content, child pornography, or content on any electronic device that shows kids engaging in sexual activity.

3.2 Indian Penal Code, 1860 (IPC):

In the incident that the IT Act proves insufficient in combating cybercrimes, law enforcement agencies may resort to the following IPC sections:

- Section 292: Originally intended to address the sale of pornographic materials, it has broadened to encompass a variety of cyber offenses, including the electronic distribution of minors' sexually explicit or pornographic acts or adventures.
- Section 354C: This regulation prohibits the taking or distribution of images of a woman's intimate parts or behaviour without her consent.
- Section 354D: This section defines and deals with stalking, including both offline and online forms of cyberstalking, which is defined as the act of persistently pursuing a woman through technology.

3.3 POCSO Act, 2012:

Section 11 of the POCSO Act defines sexual harassment. Any anyone who routinely contacts a kid through internet communication or makes threatens to utilize the child's body or engage the minor in sexual activity—regardless of whether these threats are Whether it's real or imagined—it's sexual harassment. The POCSO Act's [9]Section 13 outlines the legal prohibition against using children for pornographic purposes. The Act's Section 14 describes the consequences of hiring a child in a pornographic capacity.

[9] The Protection of Children from Sexual Offences Act, 2012.

3.4 Data Protection Bill 2021:

The law affords children a number of privacy protections. The requirement that a data fiduciary obtain consent from the guardians before processing a child's personal information is among the most crucial ones. It also counsels data fiduciaries who exclusively deal with kids to create an account with the data protection regulator. Data fiduciaries are banned from surveilling, monitoring, or processing children's data in a way that could endanger the children.

The primary goal of this draught legislation, which is based on a report by a joint parliamentary committee that amends the two existing laws, is to protect children's internet privacy**.**

3.5 Digital India Bill 2023:

The purpose of this new legislation is to create thorough regulation over India's digital environment, addressing issues such as cybercrime, data security, deepfakes, platform competition, online safety, and the negative artificial intelligence's influence.

3.6 Amendments in laws to deal with cyber abuse:

The Indian Penal Code, 1860 Prior to 2013, no law directly dealing with online harassment or crimes pertaining to women in the cyber space. The 2013 Criminal Amendment Act to the Indian Penal Code, 1860 by way of Section 354A to Section 354D

IT Act Amendment 2000

4. Conclusion:

Child cyber abuse poses significant threats to the safety of minors in Gujarat, India, necessitating urgent attention. This study has illuminated the prevalent forms of abuse and highlighted gaps in the implementation of existing legal frameworks. To address these challenges, collaborative efforts among stakeholders are essential, alongside improved data collection and targeted interventions. Enhanced awareness, robust reporting mechanisms, and capacity-building initiatives are recommended to create a safer online environment for Gujarat's children. By taking decisive action, we can work towards safeguarding the well-being and rights of the youngest members of our society in the digital age.

References:

1. Barua, A. (2018). Child Protection in India: A Historical Perspective. International Journal of Criminology and Sociology, 7, 121-134.
2. Chawla, A., & Garg, A. (2017). Cyber safety for children: A study of awareness levels among parents and guardians in India. International Journal of Engineering and Computer Science, 6(6), 21907-21912.
3. Childline India Foundation. (n.d.). About Childline. Retrieved from https://www.childlineindia.org.in/about-childline.htm
4. Government of Gujarat. (2020). The Gujarat Cyber Crime Police Station. Retrieved from https://police.gujarat.gov.in/content/police/en/gujarat-police-organization/units/cyber-crime-police-station.html
5. Ministry of Women and Child Development, Government of India. (2012). The Protection of Children from Sexual Offences Act, 2012. Retrieved from https://wcd.nic.in/act/pc-so-act-2012

6. Sharma, S., & Pandit, M. (2021). Child Online Protection: Issues and Challenges. International Journal of Human Rights in Healthcare, 14(3), 258-271.
7. Sengupta, A., & Rout, S. (2019). Child Sexual Abuse: A Review of Literature. Journal of Indian Health Psychology, 14(2), 99-109.
8. United Nations Children's Fund (UNICEF). (2020). Child Protection. Retrieved from https://www.unicef.org/india/what-we-do/child-protection.
9. Vora, N. (2017). Cyber Crime in India: A Review of Current Scenario. Indian Journal of Applied Research, 7(5), 176-178.
10. Anderson, J. (2019). "Understanding the Scope of Cyberbullying Among Children in India." Journal of Cyberpsychology and Social Networking, 12(2), 45-58.
11. Sharma, A., & Patel, R. (2020). "Impact of Cyber Abuse on Children's Mental Health: A Case Study from Gujarat." Journal of Child Psychology, 15(3), 112-127.
12. State Commission for Protection of Child Rights. (2018). Annual Report on Child Cyber Abuse cases in Gujarat.