THE REDWOOD JOURNAL

VOLUME:-1 ISSUE NO:- 1 , NOVEMBER 13, 2025

Website: www.theredwoodjournal.com

Email: theredwoodjournal@gmail.com

Authored by:- Premnath S D, Assistant Professor and Head, Global college of Arts and Science, Thiruvarur, Tamil Nadu

EVALUATING THE EFFECTIVENESS OF CYBERCRIME LEGISLATION IN ENSURING DIGITAL SAFETY FOR WOMEN AND CHILDREN IN INDIA

Abstract

Cybercrimes such as online harassment, stalking, grooming and exploitation of women and children are on the rise in India. This paper examines the role of the cybercrime laws of India, specifically the Information Technology Act of 2000, the POCSO Act and some provisions of the Bharatiya Nyaya Sanhita, in promoting digital safety. These laws do provide the legal backbone to deal with cyberstalking and child pornography but the rate of conviction is low, awareness is lacking and technological barriers render enforcement weak.

The current paper discusses the necessity of specialized cybercrime divisions, digital awareness programs, and cooperation between countries to overcome such challenges. Recommendations for changes to laws will be based on the evolving cyber threats, such as deep fakes and Artificial Intelligence misuse. The present study emphasizes the importance of improving law enforcement efforts and victim support systems to create a safer digital environment for women and children.

Keywords: Child, Women, Online, Social Media, Cybercrime, POCSO, IT Act

Introduction

Crimes are an inevitable part of the society. It started when Humans started to claim humans, Land and properties as their own. With Human evolution, the method of committing crime is also changed. We have seen various scientific innovations in the world till Today. In that, Digital transformation is also major huge step in the development. This development may have caused numerous good developments. But it also causes substantiate amount of criminal activities.

The rapid growth of digitalization caused India as a major player in the global digital resources. Some examples of Cybercrimes like online harassment, cyber pornography, cyber fraud, cyberstalking, and exploitation have become more common. Crimes involving digital, especially those that target women and children has seen a drastic rise due to the global digitalisation. It causes serious risks to the personal safety and psychological well-being of the victimised individuals of vulnerable groups such as women and children.

The recent statistics shows the severity of the Cybercrime's problem: In India in between the January and April 2024, there are over 740,000 complaints were filed on the National Cybercrime Reporting Portal, as a result of cybercriminal activities. It shows losses exceeding ₹1,750 crores were reported by the Indian citizens. This concerning trend to combat cybercrime highlights the urgent need for strong legislation and enforcement mechanisms.

There are still obstacles to overcome in order to effectively combat cybercrime because of the India inadequate current legal frameworks. Due to the day to day evolvement and development of technology, the crimes are frequently out ways the existing legistations, leaving gaps that cybercriminals take loopholes of the law and the enforcement. And also there is need for educating the public and make aware regarding cyber threats and victims support legal options.

By Assessing and analysing the India's current legal frameworks by comparing with other nation's cyber-criminal laws, and offering practical legal and societal recommendations for strengthening the digital safety measures in India. The purpose of this paper is to assess how well India's cyber related criminal laws protect women and children in the online platforms.

Research Objectives

- To assess the effectiveness of India's current cybercrime laws in protecting women and children with other nations.
- To identify challenges in the implementation and enforcement of the cyber laws in India.
- To propose recommendations for enhancing digital safety of Women and Children in India.

Definition of Cybercrime

The US Department of Justice (1989, as cited in Halder et al., 2012) defined computer crimes as “those crimes where knowledge of a computer system is essential to commit the crime” (Parker, 1989). McConnell International (2000, as cited in Halder et al., 2012) defined cybercrimes as “harmful acts committed from or against a computer or network”.

According to the council of Europe (2001, as cited in Halder et al., 2012),

> This convention presented the concept of cyber offences in five dimensions. They are (i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) Computer related offences; (iii) content related offences; (iv) offences related to infringements of copyright; (v) abetting or aiding such offences.
>
> The first group, i.e., offences against the confidentiality, integrity and availability of computer data and systems included the following:
>
> (a) Intentional illegal access to the whole or any part of the computer system by infringing security measures. The motive could be either to obtain computer data, or any other dishonest intention, or illegal access in relation to a computer system that is connected to another computer;
>
> (b) Intentional illegal interception without any proper rights whatsoever, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data;
>
> (c) Intentionally interfering with the data without any proper rights what so ever;

(d) System interference, i.e., hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;

(e) Misuse of devices; this includes the production, sale, procurement for use, import, distribution of a computer device or programme designed or adapted primarily for the purposes of offences mentioned above under point (a) or a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, and the possession of any of these items with a criminal intent (Council of Europe, 2001).

The second group, i.e. 'Computer related offences' would mean:

(a) computer related forgery i.e., the input, alteration, deletion, or suppression of computer data resulting in inauthentic data with the intent that it may be acted upon for legal purposes as if it were authentic for fraudulent purposes; and

(b) computer related fraud, i.e., intentionally causing of a loss of property to another person by either

(1) any input, alteration, deletion or suppression of computer data, or (2) any interference with the functioning of a computer system, or both with fraudulent purpose for procuring monetary gain for one person or for another person which deal with child pornography only. It includes procuring, making, offering, distributing and possessing child pornographic materials in the computer system or using the computer systems to do all these for the monetary gains. Child pornography is defined and described as materials that visually portray (i) an act by a 'minor', where he is engaged in sexually explicit conduct; or (ii) an act by a person "appearing" to be a minor, who is engaged in sexually explicit conduct; or (iii) realistic images representing a minor, who is engaged in sexually explicit

conduct. The Convention shows the age limit to be termed as minor, as less than 18 years. The Convention also specifies that lower age limit could be shown as 16 years in some cases.

The fourth group indicates 'Offences related to infringements of copyright', i.e., when the offence infringes the law copyrights and related rights of the member country. The last group includes aiding and abetting any or all of the cyber offences that are grouped above.

Cybercrimes against women are: "Crimes targeted against women with a motive to intentionally harm the victim, using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". (Halder etal., 2012)

Cybercrimes against child defined as offenses that are targeted against child with a motive to intentionally harm the victim, using games, social Medias etc,

Major forms of Cybercrime focusing Women and Child

Cyberstalking

It involves the use of the internet or other electronic means to stalk or harass an individual in the online platforms. Stalkers may monitor, intimidate, or threaten victims (women and children). It may to lead to severe psychological distress and fear. Women are more victimised to cyberstalking, which can continues to offline threats.

Cyberbullying

It refers to the act of posting, sending, or sharing negative, harmful, accusations, false, or mean content about the victim or someone else, typically through online platforms. Children

and adolescents are vulnerable targets of cyberbullying, leading to issues like depression, anxiety, and in extreme cases, suicide.

Online Grooming

It involves abusers befriending with the minors by gaining their trust in the intent of sexual abuse at the online platforms. This involves manipulating the child into sending explicit picture and videos of themselves and arranging face to face meetings.

Cyber Pornography and Deepfake

The creation, distribution, or consumption of explicit content without consent is known as Cyber pornography. With Innovations in technology like photo video editing and Artificial Intelligence, deepfake pornography—where individuals' faces are taken and pasted onto explicit videos—has become a growing concern, particularly affecting women who are celebrities.

Sextortion

In this, where the victims are lured into providing sexual images or favours under threat of sharing their private images of them and sensitive information about them. Both women and children can fall victim to sextortion, leading to severe psychological trauma and in case of extreme, they may commit suicide.

Cyber Defamation

It is the process of spreading false information about an personnel in the online media to damage their reputation or growth. Women often face accusation regarding their character through malicious posts, comments, or fabricated (edited) content.

Exposure to Inappropriate Content

The predator may send and force the children to sexual contents. It can cause long terms impacts on their development, following the wrong path, porn addiction and well-being.

Comparison of India's Cyber law and enforcement with other nations like United States of America, United Kingdom, Russia

Cybercrime & Punishments

Cybercrime	India (IT Act, 2000, POCSO, IT act, POSH act)	USA (CFAA, ECPA, CISA)	UK (Computer Misuse Act, GDPR)	Russia (Criminal Code & IT Laws)
Cyber Fraud	3 years jail + ₹1 lakh fine	20 years jail	10 years jail	5 years jail
Child Pornography	5 years jail + ₹10 lakh fine	30 years jail	15 years jail	10 years jail
Cyber bullying & Harassment	No specific law (only IPC 354D)	5-10 years jail	5 years jail	5 years jail

Data Theft	3 years jail + ₹5 lakh fine	10 years jail	10 years jail	7 years jail

Law Enforcement & Cybercrime Investigation

Aspect	India	USA	UK	Russia
Who Investigates?	CERT-In and Police Cyber Crime Units	FBI Cyber Crime Division, National Security Agency, Homeland Security	National Crime Agency (NCA), The National Cyber Security Centre	Federal Security Service (FSB), Cyber Police
How to Report?	Cybercrime.gov .in	IC3.gov (FBI)	Action Fraud (UK)	Reports to FSB
Jurisdiction	Cases handled by State	Federal-level prosecution	Prosecuted under UK laws	Cases handled by FSB
International Cooperation	Limited (Interpol, CERT alliances)	Strong cooperation with INTERPOL, EUROPOL	Member of Budapest Convention	Limited cooperation (cyberwarfare concerns)

Conclusion

This paper highlights the critical need for prompt and comprehensive cybercrime legislation to safeguard women and children in India. While existing legislation, such as the Information Technology Act, 2000, provide a basic legal structure. But they often fall short in

investigating and prosecuting the unique challenges posed by cybercrimes targeting these vulnerable groups. The rapid development of technology and the increasing problems of cyber threats makes continuous updates to legal provisions, improved international cooperation, and a multifactorial approach that includes public awareness, capacity building, and technological advancements. India can better protect its citizens from the various dangers of cybercrime by adaption united and adaptable legislation and it can ensure a safe digital environment for women and children.

Recommendations

- By updating the India's Information Technology Act, 2000 to address online harassment, cyberbullying, cyber pornography and cyberstalking of women and children. Similar to the practices in the USA (CFAA) and UK (Computer Misuse Act), with harsher penalties.
- Enact and enforce specialized laws for child exploitation, online grooming, and child pornography similar to the USA's Adam Walsh Act and UK's Sexual Offences Act.
- Train and deploy dedicated cybercrime units to address women and children-related cybercrimes, similar to the FBI's Cyber Crime Division in the USA and the UK's National Crime Agency (NCA).
- Improve cybercrime reporting platforms to make them more accessible, easy to report and anonymous, similar to the USA's IC3 and UK's Action Fraud. This will encourage more women and children to report cybercrimes.
- Establish specialized helplines call and units and support systems for cybercrime victims, offering legal assistance and psychological support.

- Launch cyber awareness programs and new initiatives focusing on women and children's digital safety, inspired by global initiatives
- Include digital safety lessons in school curriculums like case studies, stories, poem to teach children how to protect themselves online and recognize threats, following the UK's school cyber programs.
- Improve international collaboration with global organizations like INTERPOL and EUROPOL to tackle international cybercrimes affecting women and children, similar to practices in the USA and UK.
- Adopt stricter cross-border laws for data protection and cybercrimes targeting vulnerable populations with global cooperation to prevent exploitation.

References

- Barman, S. & Raiganj University. (2024). Cybercrime against Women : How cybercrime targets women's privacy and security. In *East Indian Journal of Social Sciences*.
- Halder, D., 1975-, Jaishankar, K., International Institute of Justice and Police Sciences, Centre for Cyber Victim Counselling (CCVC), India, & Manonmaniam Sundaranar University, India. (2012). *Cyber Crime and the Victimization of Women: Laws, rights and regulations*. Information Science Reference (an imprint of IGI Global). https://doi.org/10.4018/978-1-60960-830-9
- P, N. N., & Jegadeeshwaran, N. D. M. (2023). An empirical study on cyber crimes against women and children in India. *International Journal of Advanced Research in Science Communication and Technology*, 141–149. https://doi.org/10.48175/ijarsct-11327

- Auwal, A. M., & Lazarus, S. (2024). Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization. *Journal of Digital Technologies and Law*, 915–942. https://www.lawjournal.digital
- AllahRakha, N. & Department of Cyber Law, Tashkent State University of Law, Tashkent 100047, Uzbekistan. (2024). Global perspectives on cybercrime legislation. *Journal of Infrastructure, Policy and Development*, *8*(10), 6007. https://doi.org/10.24294/jipd.v8i10.6007
- Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024. https://doi.org/10.31893/multirev.2025024
- Kale, M. P. (2024). The role of legal frameworks in combating cybercrime: global perspectives and local implications. *African Journal of Biomedical Research*, 186–195. https://doi.org/10.53555/ajbr.v27i5s.5149
- Tripathy, N. S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. *International Journal of Science and Research Archive*, *13*(1), 2360–2374. https://doi.org/10.30574/ijsra.2024.13.1.1919
- Pandey, P., & Kapoor, A. (2025). CYBERCRIME IN THE DIGITAL ERA: IMPACTS, AWARENESS, AND STRATEGIC SOLUTIONS FOR a SECURE FUTURE. *Sachetas*, *4*(1), 32–37. https://doi.org/10.55955/410004
- Banu, R., & Banerjee, J. (2025). Examining the role of digital forensics in strengthening cybercrime investigations in India [Article]. *International Journal of Human Rights Law Review*, *1–1*, 58–68. https://www.researchgate.net/publication/387876472
- Council of Europe. (2001, November 23). *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

- Kumar, N. (2021). CHILDREN AND CYBER CRIMES. *International Journal of Social Science and Economic Research*, *6*(4), 1324–1334. https://doi.org/10.46609/ijsser.2021.v06i04.014
- Computer Fraud and Abuse Act, 1986
- Information Technology Act, 2000
- Bharatiya Nyaya Sanhita, 2023
- Protection of Child from Sexual Offences, 2012
- Sexual Harassment of Women at Workplace, 2013
- Electronic Communication privacy Act, 1986
- Cyber security Information Sharing Act, 2015
- Computer Misuse Act, 1990
- General Data Protection Regulations, 2016