IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 10, March 2024

Impact Factor: 5.731

A Study of Cybercrime Against Women and Children in India using Noval Technology with Special Reference to Covid-19

Pratyush Kumar Chand[1] and Prof. (Dr.) Sanjaya Choudhary[2]

Research Scholar, Law Department, Bhagwant University, Ajmer, Rajasthan, India[1]

Professor, Law Department, Bhagwant University, Ajmer, Rajasthan, India[2]

Abstract: *India emerged as the third most vulnerable country in 2017 in terms of risk from cyber threats such as malware, spam and ransomware. Cybercrime is completely different from traditional crimes. With the emergence of technology, which is for the betterment of the society, is creating more problems especially for women. We can see cases of cyber trolling on social media, harassment through e-mail etc. as an aspect of cybercrime against women. India has also made a separate law to prevent cybercrime against women. The Information Technology Act 20003 seeks to effectively prevent cybercrimes against women. Cybercrime in the broadest sense means any illegal behavior through or in relation to a computer system or network, including crimes such as illegally possessing and introducing or distributing information using a computer system. Cybercrime first started with hackers trying to break into computer networks. Some did so simply for the thrill of accessing high-level security networks, but others tried to obtain sensitive, classified material. Ultimately, criminals began to infect computer systems with computer viruses, causing personal and business computers to malfunction. With the advent of computers in the late 1960s, crimes were mostly related to physical damage to computer networks and telephone networks. The COVID-19 pandemic has accelerated the digitalization of daily life, leading to an increase in online activities, distance learning, and virtual communication. However, this rapid change has also exposed women and children to new and intensified forms of cyber exploitation, harassment and abuse. The study explored various manifestations of cybercrime, including online harassment, sextortion, and the distribution of explicit material, with a particular focus on the unique challenges posed by the pandemic. The research includes analysis of innovative technologies such as artificial intelligence, deepfakes and blockchain, examining their role in enabling and combating cybercrime. Additionally, legal frameworks and law enforcement responses are examined to assess their effectiveness in combating emerging cyber threats. The study aims to identify gaps in existing regulations and propose innovative solutions to increase legal and technical resilience against cybercrime.*

Keywords: COVID-19, Cyber Crime, Deepfakes and Blockchainetc

I. INTRODUCTION

Internet is one of the most important inventions in the communication field with the help of which, people living all over the world can communicate with each other without realizing the distances between them.[1] It has reduced the boundaries between people and provided them with opportunities to build better relationships on both personal and professional fronts. The number of social network users in India has increased significantly, from 181.7 million in 2015 to 216.5 million in 2016 and an estimated 250.8 million in 2017. However, on one hand it is a boon, but on the other hand it has created insecurity in the lives of women due to increasing criminal activities in the virtual world. With the emergence of the Internet the safety of women of all ages and backgrounds is in a vulnerable state. Women are

1Leonard-Barton, Dorothy, and Kraus, William A.. Implementing New Technology. United States, Harvard Business School Reprint, 1985.

IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 10, March 2024

Impact Factor: 5.731

particularly vulnerable to cybercrime and harassment, which poses a serious threat to personal security. Although the number of internet users in India is increasing day by day, there is also some gender disparity that is clearly visible among social network users. This can be seen in various areas such as the number of people using the internet as well as the number of people using Facebook or Twitter or Instagram etc. The unbalanced number of users on the Internet is a major contributor to this phenomenon. This has a deep connection with the increasing incidents of cybercrime against women and children. Talking about the legal framework in India to deal with cybercrimes, essentially, there are two paradigms that address cybercrimes against women and children. Namely, they are the Indian Penal Code, 1860 and the IT Act, 2000. The IPC does not specifically talk about cybercrimes, rather it is a general criminal law, which defines various crimes and specifies the punishment to be given for those crimes. , It should be borne in mind that the crimes listed in the Code are addressed to the physical or tangible or their commission in the real world. The provisions of the IPC are relevant to cyber violence against women through legislative amendments and judicial interpretations. The IT Act majorly covers commercial and economic crimes but there are no specific provisions to cover cybercrimes against women. Access to the Internet is a need of every individual and hence, it is fast becoming a necessity for financial prosperity and is being seen as a basic human right. Thus, it is important to ensure that this digital public space is a safe and enabling space for everyone, including women of all ages.

Internet usage has increased during lockdown across the world. With nowhere to go, people are at home. Social media usage is at an all-time high, with the majority being from the younger generations i.e. Millennials and Gen Z. With limited digital literacy, people are finding it difficult to navigate in daily life. Cyber harassment of sexual minorities and minors has been a major issue during this period. In the case of minors, it also stems from the fact that they are not aware of their rights in cyberspace, even if they are proficient in using the Internet. In some cases, they may also become victims of cybercrimes like cyberstalking, cyberbullying, child pornography, etc. This article discusses these crimes, with special reference to cybercrimes against women and the increase in them during COVID-19. This article will also throw light on the Information Technology Act, 2000 along with important steps that can be taken to prevent cybercrimes.

1.1 What is cybercrime?

Cybercrime refers to criminal activities conducted via the Internet or otherwise conducted by computer technology, such as using online social networks to harass people or share sexually explicit photographic files. Although cybercrime is a new problem, many crimes committed over a computer or smartphone, such as theft or child pornography, were committed in person before the computer age. This paper includes information about catfishing, stalking, child pornography and many other crimes committed online.

1.2 Types of cybercrimes against women

Cyber stalking

Cyberstalking is one of the most common crimes committed by cybercriminals. Stalking refers to an attempt to contact/locate a person through his online details without his consent or after he has refused to disclose the said information. This is done through e-mails, mailing lists, hacking of personal data, image searches, etc. To understand, we will classify stalking in three ways, namely email stalking/internet stalking, threats and physical stalking.

Sending objectionable material: Continuous sending of obscene material, messages, photos to harass the victim through email/social media profiles/messaging apps.

Threats: Publishing obscene material to blackmail, intimidate or 'outrage the modesty' of a woman. In such a situation, Section 354D of IPC can be used against the criminal.

Physical Stalking: Using the above means, criminals can also gain access to personal information like place of residence, place of work, usual mode of transportation which can later lead to physical stalking.

Revenge porn

Revenge pornography is an illegal act that involves publishing, broadcasting, creating or displaying obscene material related to a woman on the internet. The use of Photoshop has added a new dimension to this issue. The photographs and

IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 10, March 2024

Impact Factor: 5.731

videos tampered with the contact details of the victim are published on the internet which not only tarnishes their reputation in the society but also affects their future. After such incidents, an increase in the unwanted advances of miscreants has also been seen.

Cyber-bullying

Cyberbullying is bullying that occurs through the use of digital technology. This can happen on social networking sites, chat systems, gaming platforms and mobile phones. Its purpose is to scare, anger, or embarrass the targeted people. Teenagers aged 14-18 years are mainly harassed by cyber criminals. Some types of cyberbullying are:

1. Catfishing: Using a made-up or stolen ID to defraud other users. This is a method often employed by scammers to create deep emotional connections with users in order to use emotional attachment for illegal purposes. This can often lead to 'tricking' which involves collecting personal information of users such as personal photographs, documents and bank information, which is often used to blackmail those individuals.

2. Frapping: When a person leaves their social media profile signed in and unattended, it leaves it open for someone else to edit their status updates in a humorous or embarrassing way. This may seem harmless, but bigger issues can arise when these changes are made by a person attempting to harm someone's reputation.

Child pornography

Publishing, creating, viewing or displaying any obscene material involving children engaged in sexual acts is illegal in India and is a serious cybercrime. Most children between the ages of 14-18 become victims of child pornography.

1.3 Punishment of cybercrimes against women and girls[2]

For easy access, here is a list of punishments for cybercrimes against women and children.

1.3.1 Indian Penal Code,1860

Prior to 2013, there was no specific law for crimes against women through the internet. But, in the year 2013, the criminal amendment act added to the Indian Penal Code,1860 included certain sections related to cybercrimes against women under sections 354A to 354D:

Section	Term of punishment
354A – Committing acts like demanding sexual favours, showing pornography without the will of women or making sexually coloured remarks	Rigorous imprisonment extended up to 3 years or with fine or with both.
354C – Commits 'voyeurism' defined as capturing images/ videos of women engaging in private acts and disseminating such material without her consent.	Imprisonment up to 3 years +fine for first conviction 3 to 7 years+fine for second and subsequent convictions.
354D – Cyber Stalking	Imprisonment up to 3 years +fine for first conviction 3 to 7 years+fine for second and subsequent convictions.
499 – Cyber Defamation	Imprisonment extended up to 2 years or with fine or with both.
509 – Outrage of women modesty	Imprisonment up to 3 years +fine

1.3.2 Information Technology Act, 2000

According to the Information Technology Act,2000 and its amendment, there are some of the sections talks about punishments of cybercrimes are as follows:

[2] https://blog.ipleaders.in/a-study-of-cybercrimes-against-women-and-girls-during-covid-19/

IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 10, March 2024

Impact Factor: 5.731

Section	Term of punishment
66C – Identity theft	Imprisonment up to 3 years +fine may extend to one lakh rupees.
66D – Cheating by impersonation using computer resources or communication devices	Imprisonment up to 3 years +fine may extend to one lakh rupees.
66E – Violation of the privacy of a person	Imprisonment up to 3 years or with a fine not exceeding two lakh rupees.
67 – Publishing obscene material through electronic form	Imprisonment up to 3 years +fine which may extend to five lakh rupees for first conviction 3 to 5 years+fine which may extend to ten lakh rupees for second and subsequent convictions.
67A – Publishing sexually explicit material through electronic form	Imprisonment up to 5 years +fine which may extend to five lakh rupees for a first conviction 5 to 7 years+fine which may extend to ten lakh rupees for second and subsequent convictions.
67B – Publishing sexually explicit material through an electronic form that depicts children	Imprisonment up to 5 years +fine which may extend to five lakh rupees for a first conviction 5 to 7 years+fine which may extend to ten lakh rupees for second and subsequent convictions.

Cybercrime is a crime committed anonymously by any person under the cover of the Internet[3]. Technology allows criminals to act anonymously and gives them access to large, vulnerable populations, including children. Teenagers around the world addicted to social media platforms like WhatsApp, Facebook, Instagram and Snapchat are easy targets for cybercrime perpetrators. While children are often unaware of the dangers associated with cyberspace, parents find it difficult to protect them from cybercrimes as they lack awareness of the legal remedies available under national and international law.[4]

Although cybercrimes against women and children have become a common phenomenon, it should not be normalized. India is one of the few countries to have enacted an Act for the Prevention of Cyber Harassment, however, its implementation is not good enough. Along with people's responsibility to keep themselves safe, we must also focus on the government's responsibility to ensure that criminals are punished and victims get justice. In crimes where marginalized communities and minors are targeted, awareness and employment of good law is irreplaceable.

1.4 Result Analysis

India decided to go digital, which gave new strength to the country. People use the Internet to discover new things and make their lives more convenient. There are no limits to who they can talk to and where in the world they can go. Cyber thieves now have new ways to operate, and most of their victims are women and children. This has become a major problem for law enforcement in the country and women and children remain at risk. Criminals in India are increasingly using the internet as a means to snoop on, harass and abuse women and children in the country. This research project will investigate “Cybercrimes against Women and Children in Covid-19” in India. The Information Technology Act of 2000 was enacted due to the rapid advancement of computer technology.The result analysis oncybercrime against women and children in India using new technology, especially in the context of COVID-19, is warranted by several urgent needs and concerns:

Escalating Threat Scenario:

A significant increase in the prevalence of cybercrimes against women and children has been observed, necessitating a thorough examination of the emerging threat landscape. The unique challenges posed by the COVID-19 pandemic,

[3] Khan, Mohammad Ayoub, et al. Cybercrime, Digital Forensics and Jurisdiction. Germany, Springer International Publishing, 2015.

[4] Power, Andrew, and Kirwan, Grainne. The Psychology of Cyber Crime: Concepts and Principles. Ukraine, Information Science Reference, 2012.

coupled with rapid advancements in innovative technologies, require a comprehensive understanding to formulate effective preventive measures.

Impact of Covid-19:

The ongoing COVID-19 pandemic has accelerated the adoption of digital platforms, as well as increased cyber threats. The result analysisaddresses the critical need to assess the specific impact of the pandemic on cybercrimes against women and children, providing insights into emerging patterns and vulnerabilities.

Innovative Technologies and Exploitation:

The misuse of innovative technologies, including deepfakes, artificial intelligence and blockchain, in cybercrimes against vulnerable populations is a growing concern. There is a need to explore the role of these technologies in facilitating cyber exploitation, understand their methods and formulate strategies to effectively mitigate the risks.

Legal Framework Assessment:

Existing legal frameworks may not be equipped to handle the rapid growth of cybercrimes. A thorough assessment of the legal mechanism is important to identify shortcomings, inadequacies and areas for improvement in protecting the rights and well-being of women and children in the digital sphere.

Technical Security Measures:

With the proliferation of innovative technologies, the need for advanced technological security measures is paramount. The objective of the proposed work is to identify and recommend innovative solutions, tools and approaches to strengthen cyber security while providing strong protection against emerging cyber threats.

Psychological and socio-economic implications:

Cybercrimes have a deep psychological and socio-economic impact on victims. Understanding and documenting these consequences is essential to creating effective support systems, counseling services and policy measures to deal with the consequences of cyber exploitation.

Empowerment through awareness:

Awareness and education play a vital role in empowering women and children to navigate safely in the digital landscape. The result analysis assesses the effectiveness of existing awareness campaigns and educational initiatives, providing insights to improve and tailor these efforts for maximum impact.

Policy Relevance:

The research findings will have direct policy relevance, informing lawmakers, government agencies, and advocacy groups about the specific challenges faced by women and children in the context of cybercrimes. This, in turn, can contribute to the formulation of targeted policies and legal reforms.

Global Relevance and Knowledge Gap:

The proposed work addresses a significant knowledge gap in the global understanding of cybercrimes against women and children, particularly in the context of new technologies and the COVID-19 pandemic. This research will contribute to the global discussion on cyber security, providing insights applicable beyond India's borders.

The result analysis is not only timely but also important to develop a holistic and nuanced understanding of the challenges posed by cybercrimes against women and children in the digital age, thereby ensuring that effective measures are taken to protect Preventive measures, legal frameworks and support systems should be developed. The rights and welfare of the most vulnerable members of society.

1.5 Conclusion

The prevalence of cybercrimes against women and children has seen a significant increase during the COVID-19 pandemic, reflecting the growing reliance on digital platforms for work, education, and social interaction. The pandemic has created a favorable environment for cybercriminals to exploit vulnerabilities, especially among vulnerable groups. Here are the key factors contributing to the prevalence of cybercrimes against women and children during COVID-19: increased online presence, distance learning challenges, increase in phishing and social engineering, online harassment and exploitation,Healthcare scams, increased use of social media, economic exploitation, gaps in cyber security awareness, privacy concerns along with remote work and education.India decided to go digital, which

gave new strength to the country. People use the Internet to discover new things and make their lives more convenient. There are no limits to who they can talk to and where in the world they can go. Cyber thieves now have new ways to operate, and most of their victims are women and children. This has become a major problem for law enforcement in the country and women and children remain at risk. Criminals in India are increasingly using the internet as a means to snoop on, harass and abuse women and children in the country. This research project will investigate "Cyber Crimes against Women andChildren in Covid-19" in India. The Information Technology Act of 2000 was enacted due to the rapid advancement of computer technology.

The main objectives of the proposed research work are as follows:

1. To understand the meaning of cybercrime against women and children.
2. To find out the reasons behind oppression of women and children.
3. To analyze the law related to preventing cybercrimes against women and children in India and find out the loopholes, if any.
4. To analyze how the COVID-19 pandemic has affected the frequency and sophistication of cybercrimes against women and children, given the increased reliance on digital platforms during the pandemic.
5. To find out the difference between legal actions and innovative technological advancements.

The proposed research on cybercrime against women and children in India using new technology, especially in the context of COVID-19, is warranted by several urgent needs and concerns:

Escalating Threat Scenario;
Impact of Covid-19;
Innovative Technologies and Exploitation;
Legal Framework Assessment;
Technical Security Measures;
Psychological and socio-economic implications;
Policy Relevance;
Global Relevance and Knowledge Gap.

REFERENCES

[1]. Hassan, F. M., Khalifa, F. N., El Desouky, E. D., Salem, M. R. and Ali, M. M. 2020. Cyber violence pattern and related factors: Online survey of females in Egypt. Egyptian Journal of Forensic Sciences 10: 6. https://doi.org/10.1186/s41935-020-0180-0

[2]. Singh, P. 2018. Cybercrime against women in India. PhD diss., Banaras Hindu University, India.

[3]. Halder, D. and Jaishankar, K. 2016. Cybercrimes against women in India. New Delhi: SAGE Publications.

[4]. Saxena, P., Kotiyal, B. and Goudar, R. H. 2012. A cyber era approach for building awareness in cyber security for educational system in India. International Journal of Information and Education Technology 2 (2): 167–170.

[5]. Sankhwar, S. and Chaturvedi, A. 2018. Woman harassment in digital space in India. International Journal of Pure and Applied Mathematics 118 (20): 595–607.

[6]. Saravanan, S. 2000. Violence against women in India. A literature review. New Delhi: Institute of Social Studies Trust (ISST).

[7]. Sarkar, S. and Rajan, B. 2021. Materiality and discursivity of cyber violence against women in India. Journal of Creative Communications. https://doi. org/10.1177/0973258621992273

[8]. Shan-A-Khuda, M. and Schreuders, C. 2019. Understanding cybercrime victimization: Modelling the local area variations in routinely collected cybercrime police data using latent class analysis. International Journal of Cyber Criminology 13 (2): 493–510.

[9]. Barker, K. and Jurasz, O. 2019. Online misogyny: A challenge for digital feminism? Journal of International Affairs 72 (2): 95–114.

[10]. Yar, M. and Drew, J. M. 2019. Image-based abuse, non-consensual pornography, revenge porn: A study of criminalization and crime prevention in Australia and England & Wales. International Journal of Cyber Criminology 13 (2): 578–594.

[11]. Luong, H. T., Phan, H. D., Chu, D. V., Nguyen, V. Q., Le, K. T. and Hoang, L. T. 2019. Understanding cybercrimes in Vietnam: From leading-point provisions to legislative system and law enforcement. International Journal of Cyber Criminology 13 (2): 290–308. https://doi.org/10.5281/zenodo.3700724

[12]. Banerjee, S. and Singh, A. 2021. Media sensitivity towards cybercrimes against women. Indian Journal of Gender Studies 28 (3): 453–461. https://doi. org/10.1177/09715215211030543

[13]. Chakraborty, C., Afreen, A. and Pal, D. 2021. Crime against women in India: A state level analysis. Journal of International Women's Studies 22 (5): 1–18.

[14]. Mondal, D. and Paul, P. 2021. Associations of power relations, wife-beating attitudes, and controlling behavior of husband with domestic violence against women in India: Insights from the National Family Health Survey–4. Violence Against Women 27 (14): 2530–2551. https://doi.org/10.1177/1077801220978794

[15]. Ravindran, S. and Shah, M. 2020. Covid-19: 'Shadow pandemic' and violence against women. Ideas for India, 17 September 2020. https://www.ideasforindia.in/topics/ poverty-inequality/covid-19-shadow-pandemic-and-violence-against-women.html (accessed 25 October 2021).

[16]. Vakul Sharma and Sheema sharma "Information Technology law and practice" 6th Edition, 2018 Universal Law Publishing Co. (lexis Nexis).

[17]. Nandan Kamath, "Law relating to computers Internet and E- commerce" Universal Law Publishing 5th Edition (2016).

[18]. Rohas Nagpal, "Commentary on THE INFORMATION TECHNOLOGY ACT, 2000 (No.21 OF 2000) (2014)

[19]. Prof. S.N. Mishra- "Indian Penal Code, As Amended by The Criminal Law (Amendment)Act, 2018", 22nd edition, 2020, Central Law Publications, Allahabad.

[20]. Prof. S.N. Mishra, "The Code of Criminal Procedure, As Amended by the Criminal Law (Amendment) Act, 2018 with Probation of offenders Act and Juvenile Justice(care and Protection of Children) Act, 2015," 22nd edition, 2020, Central Law Publications, Allahabad.

[21]. Dr. Avtar Singh, "Principles of the Law of Evidence", 20th edition, 2013, Central Law Publications, Allhabad.

[22]. V.N. Shukla, "Constitution of India"-11th edition 2007 eastern book Company Lucknow.

[23]. M.P Jain –"Indian Constitutional law" 6th edition 2012, lexis Nexis Nagpur.

[24]. Dr. J.N. Pandey- "Constitutional Law of India", 44th edition 2007 central Law Agency, Allahabad.