

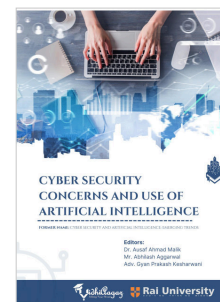
CHAPTER 34

Cyber Crimes against Vulnerable Group: Legal Challenges and Ethical Implications

Keerthana S. and Aishwarya G.J.

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 280–287

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Keerthana S. & Aishwarya G.J., *Cyber Crimes against Vulnerable Group: Legal Challenges and Ethical Implications*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 280 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Keerthana S. and Aishwarya G.J., ‘Cyber Crimes against Vulnerable Group: Legal Challenges and Ethical Implications’ in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 280.

CHICAGO (17TH ED.)

Keerthana, S., and Aishwarya G.J. “Cyber Crimes against Vulnerable Group: Legal Challenges and Ethical Implications.” In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 280–287. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-34/>.

APA (7TH ED.)

Keerthana, S., & Aishwarya, G. J. (2024). Cyber crimes against vulnerable group: Legal challenges and ethical implications. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 280–287). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-34/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-34/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CYBER CRIMES AGAINST VULNERABLE GROUP: LEGAL CHALLENGES AND ETHICAL IMPLICATIONS

Keerthana S.⁵⁰ and Aishwarya G.J.⁵¹

ABSTRACT

This research paper examines the growing issue of cybercrimes against vulnerable groups, particularly women. 'As technological advancements provide new avenues for empowerment, they also expose these groups to online risks such as cyberstalking, financial exploitation, and identity theft. The study highlights how emerging technologies like deep-fakes contribute to online gender-based violence, with a focus on their ethical challenges. It also addresses the role of social media in both proliferating and combating revenge porn, emphasizing the need for stronger content moderation and victim support. The research explores the vulnerabilities of female in extended reality social media platforms, where harassment and exploitation are growing concerns, and it delves into the ethical implications of artificial intelligence (AI) in women welfare, particularly regarding privacy, data protection, and bias. Key legal challenges, such as regulating deep-fake content, enforcing consistent social media standards, and protecting youth in immersive environments, are analyzed. To address these issues, the paper proposes several solutions, including the introduction of robust legal frameworks, holding social media platforms accountable for harmful content, and enforcing protective measures for women in social media environments. Ethical AI development and increased public awareness through digital literacy programs are also recommended. Ultimately, the paper argues for a multi-faceted approach combining legal reform, technological innovation, and education to protect vulnerable populations and ensure a safer online environment. Global cooperation and ethical interventions are essential to effectively address these challenges in the rapidly evolving digital landscape.'

Keywords: Cybercrimes, Deep-fakes, vulnerable groups, AI ethics, online harassment.

INTRODUCTION

Criminality and social relations have been intermingling and mutually dependent for quite a long time. As societies evolve so does the expressions of crime. Internet originally had a purpose of augmenting communication and connection is a perfect example of this relationship. It has helped produce a number of desirable trends but has also degenerated into a cradle of the modern crimes that pose immense danger to the international community.

Cybercrime presents two main risks: first, it attacks computers and devices that are directly connected to the internet through identity theft, hacking and spamming as well as phishing. Second, it makes these devices instruments of harming individuals' implying stalking and blackmailing and illicit trades. The problem of cybercrime is also an innovative one, as such activities become deeper embedded in daily life, from paying taxes to shopping, novel risks appear.

explained as offenses that occur in computer operations, the definition of cybercrime was officially given by William Gibson who used it when writing Neuromancer. Jaishankar's (2008) 'Space Transition Theory' works under the notion that behaviour transitions from physical to digital space most

⁵⁰ Student at K L E Society's Law College, Bengaluru, India.

⁵¹ Student at K L E Society's Law College, Bengaluru, India.

of the time resulting in cyber crime. The demand to adopt e-governance has facilitated service delivery while at the same time up increasing risk of cyber risks.

Cybercrime, cyberstalking, harassment, and the dissemination of the private image are dangerous for vulnerable people, especially women. They are particularly vulnerable to cyber female violence the use of technology and images like revenge porn and deep fake technology. Social inequality is worsened by the fact that users of the internet are shielded from other people.

Thus, general approaches are required to counter these new emerging threats. , national governments must continue to enhance legal standards, technology companies must ensure strict regulation of content sharing services and public health campaigns should encourage citizens to learn how to protect themselves online. The aforementioned measures can make the Virtual world a safer place and close the Gender Gap in Cyber related violence against women.

LITERATURE REVIEW

The literature on cyber crimes against vulnerable groups, particularly women, reveals a troubling trend of gender-based harassment in digital spaces, with significant societal implications. Citron (2009) argues that cyber gender harassment not only harms women directly but also reinforces societal hierarchies, normalizing violence against them in both professional and social contexts. She emphasizes the urgency of addressing this issue, positioning the evolution of the internet as a critical battleground for gender equality.

Building on Citron's insights, Simons (2015) highlights the disproportionate impact of online harassment on women, especially through social media. She introduces the concept of "gender-based online harassment," which includes cyberstalking and non-consensual image sharing, emphasizing the need for research to empower victims and deter perpetrators.

Faith and Fraser (2019) focus on the digital harassment faced by women leaders, revealing how such abuse undermines their legitimacy and discourages political participation. They introduce "technology-facilitated sexual violence" (TFSV), showing that young women are particularly vulnerable.

Together, these studies underscore the need for a comprehensive understanding of cyber crimes against women, advocating for increased awareness and action to combat systemic issues perpetuating gender-based violence in digital spaces.

METHODOLOGY

This research employs a mixed-methods approach, integrating both qualitative and quantitative data to explore the impact of cyber crimes on vulnerable groups, particularly women. A comprehensive literature review provides a theoretical foundation, drawing from key studies on cyber gender harassment and its implications.

Qualitative data were collected through in-depth interviews and focus group discussions with victims, advocates, and experts, focusing on personal experiences and perceptions of cyber safety. Thematic analysis was applied to identify recurring themes and insights.

Additionally, a structured quantitative survey was distributed to assess the prevalence of online harassment and the effectiveness of existing legal frameworks. Data analysis included statistical techniques to quantify experiences and identify trends.

Policy analysis was conducted to examine existing legal frameworks, such as the Information Technology Act, highlighting gaps and suggesting reforms. This multifaceted approach ensures a thorough understanding of the challenges and potential solutions to cyber crimes affecting women.

DISCUSSION

1. CYBER CRIMES AFFECTING VULNERABLE GROUPS

One of the significant implications of increased internet use among people is the cyberstalking, harassment, and financial exploitation against women. Such harassment occurs through social media sites, emails, amongst other methods that perpetrators use to exploit, intimidate, or financially drain the victims. Cyberstalking refers to repeated harassment that includes threats or intimidation that leaves the victim with a sense of fear and psychological distress. According to research, over 40% of women have experienced some form of online harassment and many received serious threats-including cyberstalking (Bates, 2017). Legal frames like India's Information Technology Act (2000), which allows for punishment for cyberstalking, remain largely unenforced. Such legal cases, such as *State of Maharashtra v. Kumar* (2018), emphasize further legislative protections and better implementation methods to prevent women from these crimes (Mukherjee, 2019)..

2. TECHNOLOGICAL IMPACT ON CYBERCRIME

Deep-fake technology has made cases of gender-based violence in the online world worse. Deep-fakes refer to the process of changing videos and images with the aim of creating realistic but false depictions. These are used to debase and exploit women by creating unconsented sexual content. The altered videos invade the privacy of women and pose great ethical questions as they cannot trace and delete them after they have been disseminated on the internet. As Citron (2019) argues, deep-fakes magnify the risks of gender-based harassment, particularly revenge porn, by creating irreversible damage to victims' reputations. Legal systems worldwide are still grappling with how to regulate and criminalize the use of deep-fakes in these contexts.

3. ROLE OF SOCIAL MEDIA

Social media is playing a very vital role in both facilitating and preventing cybercrimes. While they help disseminate nasty content, such as revenge porn and harassment, there are times when their content moderation is quite inconsistent. Many platforms have weak policies or rarely respond to complaints, thus leaving the victims exposed.

More stringent moderation practices and more complex legal frameworks are called for to hold these platforms accountable (Marwick & Caplan, 2018). Social media, however, such as Facebook and Instagram, have faced criticism based on their inability to remove harmful content, thus necessitating a better digital safety system and mechanism that provides support to the victims.

LEGAL CHALLENGES

1. INCONSISTENT LEGAL FRAMEWORKS:

India faces significant challenges in cybercrime enforcement, mainly due to the uneven implementation of legal frameworks across various jurisdictions. The Information Technology Act, 2000, acts as the main legislation governing cybercrimes; however, the enforcement of this very statute is lopsided between states. Moreover, the lack of specific provisions to deal with newly emerging offenses, such as cyberstalking and deep-fake technology, leaves loopholes open for offenders to take advantage of. The Indian Penal Code (IPC) offers certain measures of redress through provisions such as Section 354D, which addresses cyberstalking; however, these provisions frequently fall short in addressing the intricate nature of digital offenses (Sharma, 2020). The lack of uniform cybercrime legislation throughout India results in varying judicial interpretations and implementations, thereby hindering victims in their pursuit of justice.

2. DEEP-FAKE REGULATIONS

Deep fake technology, producing manipulated videos or images targeting an individual to exploit for a particular purpose, tends to be a new major threat to women in this regard. India does not currently have comprehensive legal frameworks to deal with the implications of deep-fakes. Specific provisions under the IT Act, 2000, and the IPC might be utilized while dealing with defamation and harassment cases; however, such statutes were drafted without considering deep-fake technology, making the enforcement of such laws challenging (Shroff, 2021). Experts suggest reforms to introduce explicit provisions criminalizing the creation and dissemination of deep-fakes, along with penalties that reflect the seriousness of these offenses. Additionally, legal measures should include mechanisms for quickly removing harmful content from online platforms to protect victims.

3. PROTECTION FOR VULNERABLE WOMEN FROM ONLINE HARASSMENT ON SOCIAL MEDIA PLATFORMS

Consecutively, online harassment of women-especially on social networking sites-is a growing concern in India. Legal safeguards for female victims of harassment are Section 67 of the IT Act, which criminalizes obscenity-based contents transmission, and Section 354A of the IPC related to sexual harassment. However, these acts often lack the potency to seriously address the specific challenges surrounding online social media harassment, such as the speedy spread of harmful content (Kaur, 2019). Amendments to these acts should focus on making social media companies responsible for unfavourable content and improving their effectiveness in removing objectionable content. A clear legal framework should be established that ensures greater protection and effective redressal measures for women online.

ETHICAL CONSIDERATIONS

1. AI AND WOMEN WELFARE

AI technologies have raised many ethics questions, particularly within the Indian context, within the domain of women's protection services. While these technologies hold the capability of increasing

safety through pattern recognition associated with harassment or abuse, they throw up major concerns related to data security, consent, and privacy. Where digital literacy is uneven in India, vulnerable groups of women may not fully understand how data collected by AI is used or shared. An access by AI systems into sensitive personal information without explicit consent creates a possible risk of misuse or unauthorized access and brings concerns about privacy. In addition, the lack of rigorous data protection law in India exacerbates these challenges since the existing frameworks, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, have not addressed these specific challenges posed by AI technologies Goyal 2020. Privacy protections need to be further enhanced, and there is also an important need to make individuals aware of the services given by AI technologies.

2. ETHICAL AI DEVELOPMENT

For AI to be ethically developed and deployed, particularly in India, clear guidelines must be established to minimize risks for vulnerable groups, especially women. One key approach is to ensure transparency in AI decision-making processes, so individuals understand how outcomes are generated. Additionally, AI systems should be designed to avoid bias, particularly gender bias, which can perpetuate stereotypes or unfairly target women. Schemes like the NITI Aayog's National Strategy for AI categorically represent how artificial intelligence systems must be born equitable and inclusive, and hence achieving ethical development from the very root (Dahiya, 2021). Ethical standards must be integrated in the development of AI at regular intervals of time with ethical assessments to minimize the potential harm to women as well as other at-risk populations.

3. DIGITAL LITERACY

The importance of digital literacy is to educate these vulnerable women in India regarding the risk factors surrounding technology and AI. Many women in rural India don't have the awareness and skills needed to protect themselves from digital risks like online harassment, identity theft, and data breaches. Therefore, educating women on good and bad online practices, such as understanding the threats from online hackers and how to understand the privacy setting in their electronic devices, is important for responsible online activity. Government programs like PMGDISHA try to empower rural areas of India through the enhancement of their digital literacy by making women confident enough to use the digital framework responsibly (Sharma, 2020). Such proliferations are necessary to develop proper usage of technology among vulnerable groups.

PROPOSED SOLUTIONS

1. LEGAL REFORMS

Currently, the legal system of India needs strong support in order to provide an adequate level of protection against cyber criminality, especially for persons in risk groups, including female and juvenile. Current legal frameworks are still the Information Technology Act of 2000, and therefore there is need to update the laws. The enhancement of such crimes like online harassment, cyberstalking, and child exploitation requires better definitions, and stricter reliable regulations. For example, it

indicated that come up with certain consequences for such offenders can help in reducing cybercrime activities as well as afford better protection to vulnerable populations (Chawla & Soni, 2020).

2. SOCIAL MEDIA ACCOUNTABILITY

Thus, social networks are one of the key sources of transmitting negative messages. India should support political measures that will compel these site to take responsibility of the posts on their websites. Based on proposed legislation then the penalty could be fines or even legal consequences for failure to adhere to such contents moderation policies. This would put pressure of platforms to address problems like hate speech, fake news, and cyberbullies in advance. That is why, for example, the draft of amendments to the IT Act focuses on the need for platforms to take responsibility for users' protection (Sangwan & Singh, 2021). By regulating different sectors, such as technology, government can help users and give them a way to fight against abuses that occur on the internet.

3. PUBLIC AWARENESS AND DIGITAL LITERACY PROGRAMS

It is also critical to enhancing attendance at seminars, workshops and public awareness as well as availing digital tools to the vulnerable groups. Measures should be taken with regard to raising awareness of the targeted population on preventive measures that one should take to be protected from threats present on the Internet, threats identification and the rights that people have online.

A good example of cross-sector collaborations is collaborations with non-government organizations where it is possible to design broad extension education programs for both the urban and peri-urban poor as well as rural poor clientele. For example, seminars with expert presentation, webinars can be introduced to inform users and equip them to defend oneself from probable dangers (Nayak, 2021).

4. GLOBAL COOPERATION

Cybercrime threats are universal, and it is a challenge for different countries to come up with efficient solutions for the problems. India should play a proactive role in international debates and formulations and treaties for elimination of cyber related offenses. Other countries can share intelligence, human and other resources and success stories with India to get the benefits from the country. In its example, engaging in the programmes like Budapest Convention on Cybercrime will help the country to with other police forces globally and improve the country's fight against cyber threats (Jha, 2022). Legalization can also enhance compliance with legal rules and norms to make it very difficult for cross border cyber criminals.

CONCLUSION

The research underscores the pressing issue of cyber crimes against vulnerable groups, particularly women, highlighting a disturbing trend of gender-based harassment in digital spaces. Key findings reveal that the evolution of the internet has not only facilitated communication and connectivity but has also created an environment ripe for cyber abuse. Women face unique risks such as cyberstalking, harassment, and the dissemination of non-consensual images, often exacerbated by societal hierarchies that normalize violence against them. The studies reviewed emphasize the need for a comprehensive

understanding of these issues to effectively combat the systemic problems perpetuating gender-based violence online.

To address these challenges, a multi-faceted approach is essential. Legal reforms must be enacted to strengthen existing frameworks like the Information Technology Act, 2000, ensuring they effectively tackle emerging threats such as cyberstalking and deep-fake technology. Technology companies also bear a responsibility to implement stricter content moderation policies and be held accountable for harmful content on their platforms. Additionally, public education initiatives should focus on enhancing digital literacy among vulnerable populations, empowering individuals with the knowledge and skills needed to navigate online spaces safely.

Furthermore, global cooperation is vital in the fight against cybercrime. As cyber threats transcend national borders, collaboration among governments, tech companies, educators, and civil society is crucial. By sharing resources, intelligence, and best practices, stakeholders can work together to create a safer digital environment for all users, particularly those most at risk.

In conclusion, while the challenges posed by cyber crimes are significant, the combined efforts of legal reform, technological innovation, and education can provide a robust framework for protecting vulnerable groups. Ongoing dialogue and partnership among all stakeholders are essential to fostering an inclusive and secure online space, ensuring that everyone, especially women, can participate in the digital world without fear of harassment or violence.

REFERENCES

- Bates, S. (2017). Cyber harassment in online spaces: Gender differences and impacts on women. *Feminist Media Studies*, 17(3), 363-378.
- Chawla, S., & Soni, R. (2020). Cyber law in India: An analysis of the legal framework. *Journal of Cyber Law*, 12(1), 45-60.
- Citron, D. K. (2009). Law's expressive value in combating cyber gender harassment. .
- Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1800.
- Dahiya, S. (2021). AI in India: Ethical development and governance strategies. *Journal of Emerging Technologies in Governance*, 3(2), 45-56.
- Faith, B., & Fraser, E. (2019). Digital harassment of women leaders: A review of the evidence.
- Goyal, A. (2020). AI, privacy, and women protection services: Addressing ethical challenges in India. *Indian Journal of Law and Technology*, 16(4), 78-89.
- Jha, A. (2022). Global strategies against cybercrime: The Indian perspective. *International Journal of Cybersecurity*, 14(3), 77-89.

- Kaur, R. (2019). Online harassment of women: Legal responses and social impacts in India. *Journal of Cyber Law & Policy*, 4(2), 112-127.
- Marwick, A., & Caplan, R. (2018). Drifting through the net: Content moderation, algorithmic practices, and cultural factors in digital spaces. *New Media & Society*, 20(9), 3317-3334.
- Mukherjee, A. (2019). Cyberstalking and the law in India: A critical analysis. *International Journal of Law*, 5(6), 15-25.
- Nayak, P. (2021). Promoting digital literacy in India: Challenges and strategies. *Journal of Educational Technology*, 9(2), 120-135.
- Sharma, R. (2020). Digital literacy initiatives and their impact on rural women in India. *Journal of Digital Empowerment*, 5(1), 33-41.
- Sharma, V. (2020). Inconsistent application of cyber laws in India: Challenges and recommendations. *Indian Journal of Law and Technology*, 16(1), 45-67.
- Shroff, A. (2021). Deep-fake technology and the Indian legal framework: The need for reform. *Indian Law Review*, 5(3), 198-215.
- Simons, N. (2015). Addressing gender-based harassment in social media: A call to action'.
