INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 3 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 3 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-3-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 3 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

VIRTUAL VIOLENCE: UNDERSTANDING CYBERCRIME AGAINST WOMEN

AUTHOR - YOGESH PRASAD KOLEKAR, ASSISTANT PROFESSOR AT M.K.E.S COLLEGE OF LAW

BEST CITATION - YOGESH PRASAD KOLEKAR, VIRTUAL VIOLENCE: UNDERSTANDING CYBERCRIME AGAINST WOMEN, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (3) OF 2025, PG. 20-23, APIS – 3920 – 0001 & ISSN - 2583-2344.

This article is published in the collaborated special issue of M.K.E.S. College of Law and the Institute of Legal Education (ILE), titled "Women's Rights and Legal Reforms" (ISBN: 978-81-968842-4-6). .

ABSTRACT

In the digital age, the internet has become an integral part of our lives, offering countless opportunities for communication, education, and empowerment. Cybercrime against women encompasses a wide range of offenses, including online harassment, stalking, defamation, morphing, revenge porn, and identity theft. Cybercrime refers to criminal activities that are executed through the use of electronic devices, such as computers or mobile phones. Cybercrime against women refers to any criminal activity that targets women using digital technologies. These crimes often exploit the anonymity and reach of the internet to harass, intimidate, or harm women. Persistent online harassment encompasses actions such as sending threatening or abusive messages, tracking a woman's online presence, or repeatedly reaching out without her permission. The act of disseminating false or harmful information about a woman across social media or other online channels is known as online defamation. India has taken significant steps to address cybercrime against women through a combination of specific laws and amendments to existing legislation. The primary legal frameworks include the Information Technology Act, 2000 and under Bharatiya Nyaya Sanhita, 2023.

Keywords: Cybercrime against women, virtual violence, cyberstalking, online defamation, Information Technology Act, 2000

Introduction

In the digital age, the internet has become an integral part of our lives, offering countless opportunities for communication, education, and empowerment. However, it has also given rise to a new form of crime cybercrime that disproportionately affects women. Cybercrime against women encompasses a wide range of offenses, including online harassment, stalking, defamation, morphing, revenge porn, and identity theft. These crimes not only violate a woman's privacy and dignity but also have long-lasting psychological and social consequences. To combat this growing menace, legal systems worldwide have introduced specific provisions to protect women from cyber exploitation and abuse.[46]

Cybercrime Against Women

Cybercrime refers to criminal activities that are executed through the use of electronic devices, such as computers or mobile phones. It includes crimes where electronic devices are

[46] YOGESH PRASAD KOLEKAR, CYBERCRIME IN INDIA: A GROWING THREAT TO CYBERSPACE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (2) OF 2025, PG. 47-29, APIS – 3920 – 0001 & ISSN – 2583-2344.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 3 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

either used as a tool for committing crime or targeted. Cybercrime against women is a significant and growing issue, encompassing a wide range of malicious activities that target women specifically or disproportionately. These crimes can have severe emotional, psychological, financial, and even physical consequences.[47]

Cybercrime against women refers to any criminal activity that targets women using digital technologies. These crimes often exploit the anonymity and reach of the internet to harass, intimidate, or harm women. Some of the most common forms of cybercrime against women include:

Cyberstalking and Harassment

Persistent online harassment encompasses actions such as sending threatening or abusive messages, tracking a woman's online presence, or repeatedly reaching out without her permission. The issue of cyberstalking and harassment directed at women is widespread and increasingly serious, particularly with the growth of digital communication and social media platforms. This behavior utilizes technology to stalk, intimidate, or threaten individuals, often resulting in significant emotional, psychological, and at times, physical harm. Women are disproportionately affected, and the repercussions can be severe.[48]

Online Defamation

The act of disseminating false or harmful information about a woman across social media or other online channels is known as online defamation. Also referred to as cyber defamation or internet defamation, this practice involves making untrue and damaging statements about an individual or organization in the digital realm. Such statements can adversely impact a person's reputation, career, or personal life, and they often circulate through social media, blogs, forums, and review sites. Unlike traditional defamation, online defamation can spread quickly and have enduring effects due to the internet's expansive reach and permanence.

Morphing and Deepfakes

The unauthorized manipulation of a woman's images or videos to produce explicit or misleading content is a growing concern. Morphing and deepfakes are sophisticated digital techniques that can generate highly realistic yet fabricated images, videos, or audio. While these technologies can serve legitimate purposes in fields like entertainment and education, they are increasingly exploited for harmful intentions, such as spreading false information, damaging reputations, or committing fraud. The use of morphing and deepfakes raises critical ethical, legal, and societal issues, especially when they are employed to harm individuals or distort public perception.[49]

Legal Provisions in India

India has taken significant steps to address cybercrime against women through a combination of specific laws and amendments to existing legislation. The primary legal frameworks include the Information Technology Act, 2000 and under Bharatiya Nyaya Sanhita, 2023

Information Technology Act, 2000

The IT Act is the cornerstone of India's legal framework for addressing cybercrimes. It includes several provisions specifically aimed at protecting women from online abuse.[50]

Section 66E

This section penalizes the violation of privacy by capturing, publishing, or transmitting a person's images in mass media without consent. The

[47] https://nluassam.ac.in/docs/Journals/NLUALR/Volume-7/Article%207.pdf
[48] https://www.verywellmind.com/what-is-cyberstalking-5181466
[49] https://www.thenewsminute.com/news/explainer-how-deepfakes-differ-from-morphing
[50] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

punishment includes imprisonment of up to three years or a fine of up to ₹2 lakh.

Section 67

This section addresses the publishing or transmission of obscene material in electronic form. The punishment for a first conviction is imprisonment of up to three years and a fine of up to ₹5 lakh. For subsequent convictions, the punishment increases to imprisonment of up to five years and a fine of up to ₹10 lakh.

Section 67A

This section deals with the publishing or transmission of sexually explicit material. The punishment includes imprisonment of up to five years and a fine of up to ₹10 lakh.

Section 67B

This section targets child pornography and sexually explicit material involving children. The punishment includes imprisonment of up to five years and a fine of up to ₹10 lakh.

Key Provisions in Bharatiya Nyaya Sanhita, 2023, related to Cybercrime Against Women

Voyeurism & Cyber Voyeurism

Section 75 (similar to IPC Section 354C)

Punishes capturing, sharing, or distributing intimate images of a woman without consent.

Punishment: 1 to 3 years of imprisonment for the first offense; 3 to 7 years for repeat offenders.

Cyberstalking & Online Harassment

Section 77 (similar to IPC Section 354D)

Punishes repeated online harassment, stalking, or monitoring a woman's digital activities.

Punishment: Up to 3 years of imprisonment and a fine.

Sexual Harassment via Digital Means

Section 73 (similar to IPC Section 354A)

Covers sending obscene messages, making unwelcome advances, or spreading offensive content online.

Punishment: Up to 3 years of imprisonment and a fine.

Defamation & Online Character Assassination

Section 354 (replaces IPC Section 499)

Criminalizes making false, damaging statements about a woman online.

Punishment: Up to 2 years of imprisonment and a fine.

Publishing or Transmitting Sexually Explicit Content

Section 163 (similar to IPC Section 292 & IT Act Section 67)

Punishes the creation, distribution, or sharing of obscene material, including morphed images or videos.

Punishment: Up to 5 years of imprisonment and a fine.

Identity Theft & Impersonation

Section 317 (similar to IT Act Section 66C)

Punishes the misuse of a woman's identity, photos, or personal data for fraud or harassment.

Punishment: Up to 3 years of imprisonment and a fine.

Conclusion

Cybercrime against women is a pressing issue that demands urgent attention. While legal provisions like the IT Act and IPC in India provide a strong foundation for addressing these crimes, their effective implementation remains a challenge.[51] Awareness, education, and empowerment are key to ensuring that women can navigate the digital world safely and

[51] Kolekar, Yogesh, A Review of Information Technology Act, 2000 (May 28, 2015). Available at SSRN: https://ssrn.com/abstract=2611827 or http://dx.doi.org/10.2139/ssrn.2611827

confidently. By strengthening legal frameworks, improving enforcement mechanisms, and fostering a culture of respect and equality, we can create a safer online environment for women and ensure that justice is served for victims of cybercrime. The fight against cybercrime is not just a legal battle but a societal one, requiring collective efforts to protect the dignity and rights of women in the digital age.[52]

Cybercrime against women is a growing and pervasive issue that poses significant threats to their safety, privacy, and mental well-being. The digital age, while offering numerous opportunities for empowerment and connectivity, has also become a breeding ground for harassment, exploitation, and abuse. Women are disproportionately targeted through cyberstalking, online harassment, doxxing, revenge porn, and other forms of digital violence. These crimes often have severe psychological, emotional, and social consequences, leaving victims feeling vulnerable and silenced.[53]

Despite increasing awareness, many women face barriers in seeking justice, including societal stigma, lack of robust legal frameworks, and inadequate enforcement mechanisms. Addressing this issue requires a multi-faceted approach, including stronger cybersecurity measures, comprehensive legislation, and public awareness campaigns to educate individuals about online safety and digital rights. Additionally, fostering a culture of respect and accountability online is crucial to creating a safer digital environment for women.[54]

Empowering women to report cybercrimes without fear of judgment, providing them with access to support systems, and holding perpetrators accountable are essential steps toward combating this menace. Governments, tech companies, and civil society must collaborate to ensure that the internet becomes a space of equality and safety for all. Only through collective effort can we hope to mitigate the impact of cybercrime against women and build a more inclusive and secure digital world.

[52] YOGESH PRASAD KOLEKAR, THE ROLE OF INDIAN CYBERCRIME COORDINATION CENTRE IN SAFEGUARDING CYBERSPACE, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (4) OF 2024, PG. 233-235, APIS – 3920 – 0001 & ISSN - 2583-2344.

[53] https://www.ijfans.org/uploads/paper/374cf990d6568e78319acc782da11df2.pdf

[54] http://ncw.nic.in/ncw-cells/legal-cell/new-bills-laws-proposed/cyber-crime-prevention-against-women-and-children-ccpwc