IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

Review on the Cyber Crime Against Women : Causes, Impact and Legal Remedies

Yogita R. Mukkanwar
Student of LL.M 2nd Year Sem IV
School of Law, Sandip University, Nashik.

Abstract: *This summary provides a comprehensive analysis of the dissertation titled "Cyber Crime and the Legal Landscape of Cyberspace," which specifically explores the intersection of information technology, criminal activity, and the vulnerabilities of women within the Indian legal context.*

Keywords: Cyber Crime and the Legal Landscape of Cyberspace

I. INTRODUCTION

The 20th century witnessed a revolution in Information Technology (IT) that fundamentally altered the global legal landscape. The explosion of the internet created challenges for lawmakers, law enforcers, and the public, as traditional legal concepts underwent a "sea-change" to accommodate the virtual world. Cyber crimes are defined as criminal activities associated with computers and computer networks through the medium of the internet. These crimes generally involve the computer as a tool, a target, or an incidental factor in the offense.

FRAMEWORK OF CONCEPT OF CYBER CRIME

The dissertation identifies a significant gap in the legal definition of cyber crimes compared to physical crimes. While physical crimes like grievous hurt or bigamy have long-established legal precedents, cyber crimes - ranging from fraud and data theft to the intrusion of privacy - pose unique challenges due to their transcendental and border less nature. The researcher emphasizes that as society becomes increasingly dependent on computers, every individual becomes a potential victim of digital illicit activity.

A primary focus of this study is the victimization of women in cyberspace. Despite India being one of the few nations to enact the Information Technology (IT) Act 2000, the dissertation argues that the specific security threats faced by women remain largely untouched by this legislation. The research utilizes a doctrinal methodology, relying on legal texts, judicial pronouncements, and statutes to evaluate the efficacy of the Indian legal regime.

II. HISTORICAL PERSPECTIVE AND CLASSIFICATION OF CRIMES

The relationship between crime and technology is not a new phenomenon; while hardware has evolved, the underlying criminal impulses remain consistent. The internet originated from a desire for a decentralized communication network that could survive a nuclear war, a project funded by the U.S. Advanced Research Projects Agency (ARPA) in the 1960s. The adoption of TCP/IP protocols in 1983 is cited as the birth of the internet, which eventually metamorphosed from a controlled military tool into a system often characterized by "anarchy". The introduction of the World Wide Web (WWW) in 1991 further globalized this reach, creating a platform for both immense social benefit and unprecedented misuse.

CATEGORIES OF CYBER CRIME :

The dissertation classifies cyber crimes into three broad categories based on the target :

1. Against Persons : Includes harassment via email, cyber-stalking, and the transmission of obscene materials.
2. Against Property : Involves unauthorized trespassing, corporate espionage, and the theft of critical information.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, May 2026 Impact Factor: 8.2

3. Against Government : Primarily concerns cyber-terrorism, which poses threats to national security and critical infrastructure, such as power grids and financial systems.

Further classification divides these acts into Violent and Non-violent offenses. Violent cyber crimes, such as cyber-terrorism and cyber-stalking, pose a psychological or physical danger to individuals. Non-violent crimes, including cyber theft, fraud, and piracy, primarily result in financial loss or social harm.

III. CRIMES SPECIFICALLY TARGETING WOMEN AND THE ROLE OF SOCIAL MEDIA

Cyberspace has emerged as a new frontier for gender-based violence. The dissertation highlights several types of crimes that disproportionately affect women :

Cyber Stalking : This involves following a person's movements across the internet, bombarding them with messages, and potentially escalating into real- world physical danger. Statistics suggest that over 75% of stalking victims are female.

Harassment via Email : This includes blackmailing, bullying, and sending unsolicited or obscene content.

Morphing : The unauthorized editing and uploading of a victim's pictures to different websites, often by creating fake profiles.

Linguistic Violence : The use of sexist jokes, demeaning acronyms, and abusive language on social media to reinforce patriarchal subordination.

THE ROLE OF SOCIAL MEDIA :

Social media acts as a "watchdog" in a democracy but also serves as a platform for victimization. It has the power to pluralize opinions and mobilize gender equality campaigns, such as those seen following the Nirbhaya case or the Aarushi murder case. However, it also facilitates "Deindividuation," where anonymity allows users to withdraw from social norms and engage in "casual sexism" and "misogyny". The researcher notes that mainstream Indian cinema often contributes to this by objectifying women, which further fuels invasive and traumatizing digital behavior.

IV THE INDIAN LEGAL FRAMEWORK (IT ACT 2000) AND ITS LOOPHOLES

The primary legislative tool in India is the Information Technology Act 2000. Its preamble indicates a focus on enhancing e-commerce, which explains why its provisions are strongest regarding commercial and financial crimes.

KEY LEGAL PROVISIONS :

Section 66 : Deals with hacking and causing damage to computer systems.

Section 67 : Addresses the publishing or transmitting of obscene material in electronic form, modeled after Section 292 of the Indian Penal Code (IPC).

Section 72 : Concerns the breach of confidentiality and privacy.

IDENTIFIED LOOPHOLES :

The dissertation argues that the IT Act is insufficient for protecting women for several reasons :

1. Lack of Specificity : The Act does not explicitly mention typical crimes against women such as cyber-stalking, morphing, and email spoofing as distinct offenses.

2. Definition of Obscenity : The Act relies on outdated standards from 1860, which do not account for modern behavior or the ease with which pornographic material is circulated today.

3. Jurisdictional Confusion : Section 75 claims extra-territorial jurisdiction if an offense involves a computer network in India, but implementing this across international borders remains a significant hurdle.

4. Under-reporting : Sociological factors, such as the fear of defamation or family dishonor, lead many women to shun the legal process entirely.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

V JUDICIAL APPROACH, FINDINGS, AND RECOMMENDATIONS

The dissertation reviews landmark cases to illustrate the judicial response to cyber crime. One notable case is Manish Kathuria v. Ritu Kohli, identified as India's first case of cyber-stalking. The accused used the victim's identity to chat online and distributed her phone number, leading to her being harassed by callers. However, the case was registered under Section 509 of the IPC (outraging the modesty of a woman) because the IT Act was not in force at the time. Another landmark is Nasscom v. Ajay Sood, where the Delhi High Court declared "phishing" to be an illegal act even in the absence of specific legislation, treating it as a form of trademark infringement and "passing off".

FINDINGS :

The researcher concludes that the existing laws relating to the "cyber" domain in India are insufficient to curb crimes against women. The penal sanctions are found to be inadequate, and there is a pressing need for a separate jurisprudence that specifically addresses virtual offenses.

MAJOR SUGGESTIONS :

Legislative Reform : Amend the IT Act to specifically define and penalize morphing, cyber-stalking, and email spoofing.

International Cooperation : Since cyber crime is global, the international community should adopt multilateral treaties similar to those used in civil aviation to ensure criminals cannot hide in "safe havens".

Capacity Building : Establish independent cyber crime investigation cells in every district and train judicial officers to handle highly technical IT offenses.

Awareness : Launch global awareness programs, treating the fight against cyber crime with the same urgency as major public health campaigns.

VI. CONCLUSION

Cyber crimes against women - including harassment, stalking, revenge porn, and identity theft are rapidly growing, fueled by increasing digital reliance and anonymity. These crimes create profound psychological distress, reputational damage, and social withdrawal. Legal remedies exist under the IT Act, 2000, and IPC (now BNS), though enforcement challenges remain.

REFERENCES

1. JuriGram, Cyberstalking & Harassment Laws in India : 2026.
2. SCC Online, Real-Life Common Cybercrimes Cases with Remedy.
3. PRS India, Standing Committee Report on Cyber Crimes and Cyber Safety of Women (2026).
4. Telegraph India, Cybercrime against women jumps to 76657 in 2025.
5. EIGE, Cyber violence against women.
6. IJCRT, Cyber Crimes Against Women In India : Types, Impact, And Legal Remedies.
7. CDR Ghaziabad, Cyber Crimes Against Women & Children