
FROM PHYSICAL TO DIGITAL VIOLENCE: REASSESSING CRIMINAL LAW PROTECTION FOR WOMEN IN INDIA

Madhushree BK, University Law College and Department of Studies in Law,
Bengaluru University, Bengaluru, Karnataka

ABSTRACT

The growth of digital technology has changed the way violence against women can happen. In the past, violence was mainly associated with places such as homes, workplaces, or public areas. Today, women may also experience abuse and harassment through social media, mobile phones, websites, and other online platforms. Traditional forms of violence, including physical violence, sexual offences, and domestic violence, are still serious concerns. However, technology has also created new forms of abuse, such as cyberstalking, online harassment, sharing private photos or videos without consent, creating fake social media accounts, and other forms of online abuse.

This paper examines whether the existing criminal laws in India are strong enough to protect women from these emerging forms of digital violence. It focuses on important legal provisions under the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and other relevant laws that offer protection to women. The study also considers the difficulties faced by the police and other authorities when dealing with online violence. These difficulties include identifying offenders, collecting and preserving digital evidence, determining which court has jurisdiction, and carrying out effective investigations.

The research uses a doctrinal legal research method. It studies existing laws, court decisions, and other legal materials to understand how Indian law deals with violence against women in both physical and digital spaces. The study identifies the gaps and practical difficulties in applying existing criminal laws to new forms of technology-based violence. Finally, it suggests ways to improve India's legal and investigative system so that women can receive stronger protection from both traditional and digital forms of violence.

Keywords: Digital Violence, Violence Against Women, Cybercrime, Online Harassment, Cyberstalking, Bhartiya Nyaya Sanhita 2023, Information Technology Act 2000, Digital Evidence, Cyber Abuse, Legal Protection, Criminal Law, Women's Safety, Online Privacy, Cyber Law.

I. INTRODUCTION

Violence against women remains a serious social and legal problem in India. Traditionally, violence against women has mainly been understood as something that takes place in physical surroundings such as the home, workplace, educational institutions, streets, or other public areas. Domestic violence, physical assault, sexual offences, and sexual harassment are some of the common forms of violence faced by women.

The growth of digital technology has changed the way such violence can take place. Today, a woman may face threats, harassment, stalking, sexual abuse, impersonation, or misuse of her personal information through social media, mobile phones, messaging applications, websites, and other online services. In many cases, the offender does not need to be physically present near the victim.

This development raises an important question for the criminal justice system: **Are India's existing laws strong enough to protect women from violence committed through digital technology?** The question is not only whether a particular offence is covered by law. It is also necessary to consider whether the police and courts can effectively investigate and prosecute such offences when offenders may use anonymous accounts, electronic evidence may be difficult to preserve, and the people involved may be located in different places.

This paper examines the changing nature of violence against women, particularly the movement from physical forms of abuse to technology-based forms of violence. It evaluates the existing legal framework, with particular attention to the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology Act, 2000 (IT Act), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA). The study also considers the practical difficulties involved in investigating digital offences and suggests measures for improving legal protection for women.

II. UNDERSTANDING DIGITAL VIOLENCE AGAINST WOMEN

Digital violence refers to harmful or abusive behavior carried out through digital devices, electronic communication, or online platforms. It can take many forms and may occur through social media, email, messaging applications, websites, or other internet-based services.

Some common examples include cyberstalking, repeated unwanted messages, online threats, sexual harassment, fake social media accounts, impersonation, online blackmail, and the

sharing of private photographs or videos without permission. Personal information may also be placed online to frighten, embarrass, threaten, or humiliate a woman.

Indian law already recognises some forms of technology-based abuse. For example, section 78 of the BNS includes monitoring a woman's internet, email, or other electronic communication as part of the offence of stalking.¹ This is important because it shows that stalking is no longer understood only as physically following someone. It can also happen through digital technology.

The IT Act also contains provisions that may apply to different types of cyber-related conduct. Sections 66C and 66D deal with identity theft and cheating through personation using a computer resource. Section 66E deals with certain violations of privacy, while sections 67 and 67A address the electronic publication or transmission of obscene and sexually explicit material.²

Although digital violence takes place online, its effects can be very real. A victim may experience fear, embarrassment, loss of privacy, damage to her reputation, emotional distress, or threats to her physical safety. Therefore, online abuse should not be treated as less serious simply because there is no direct physical contact.

III. WHY DIGITAL VIOLENCE NEEDS LEGAL ATTENTION

The internet has made communication easier and faster, but it has also given offenders new ways to target women. A person can create a false identity, use an anonymous account, repeatedly contact a victim, or distribute harmful material to a large number of people without being physically present.

The rapid spread of online information creates another serious problem. A photograph, video, message, or personal detail can be copied and shared by many people within a short period. Even when the original material is removed, copies may continue to circulate.

Digital violence can also cross geographical boundaries. For example, the victim may be in one city, the accused may be in another state, and the relevant online service or data may be located outside India. Such situations can make investigation more difficult and may raise questions about jurisdiction and access to electronic information.

For these reasons, criminal law must consider not only the nature of the harmful act but also the technology used to commit it.

IV. EXISTING INDIAN LEGAL FRAMEWORK

India has several laws that can provide protection against different forms of violence and abuse. The BNS replaced the Indian Penal Code, 1860, and contains provisions dealing with offences against women, including sexual offences and stalking.³

Section 78 of the BNS is particularly relevant to digital stalking because it specifically refers to monitoring a woman's internet, email, or other electronic communication.⁴ This provision shows that the criminal law can recognise technology as a means through which stalking may occur.

The IT Act is also important when dealing with offences involving computers and electronic communication. Section 66E deals with certain acts involving the capture, publication, or transmission of images of private areas without consent in circumstances that violate privacy.⁵ Sections 67 and 67A deal with the publication or transmission of obscene and sexually explicit material in electronic form.⁶

Another important development is the BSA, which deals with electronic and digital evidence. Section 61 recognises electronic or digital records within the evidentiary framework, while sections 62 and 63 provide rules relating to proof of electronic records.⁷

These provisions are important in cases involving screenshots, emails, photographs, videos, social media posts, electronic messages, recordings, and other forms of digital material.

Therefore, India already has several legal provisions that can be used in cases involving digital abuse. However, the existence of these provisions does not automatically guarantee effective protection. Their success depends on proper investigation, evidence collection, interpretation, and enforcement.

V. DIFFICULTIES IN INVESTIGATING DIGITAL VIOLENCE

Identifying the offender is one of the major difficulties in digital crime cases. Offenders may use fake accounts, false names, temporary phone numbers, anonymous profiles, or other

methods to hide their identity.

Digital evidence also creates challenges. Important evidence may be found in messages, emails, photographs, videos, social media accounts, device records, or other electronic information. Such material can sometimes be deleted, modified, or removed before investigators have an opportunity to preserve it.

The BSA provides rules concerning electronic and digital evidence.⁸ However, having legal rules about evidence is only one part of the problem. Investigators must also have the technical skills needed to identify, collect, preserve, authenticate, and present electronic evidence before a court.

Jurisdiction is another difficulty. An online offence may involve people located in different cities, states, or countries. The digital platform involved may also operate from another country. This can make it difficult to determine which authority should investigate the matter and how the necessary information can be obtained.

Therefore, dealing with digital violence requires both legal understanding and technical expertise.

VI. THE GAP BETWEEN TECHNOLOGY AND CRIMINAL LAW

Technology is developing very quickly. New social media platforms, communication tools, artificial intelligence applications, and other digital services continue to appear. At the same time, offenders are finding new ways to misuse these technologies.

As a result, a form of online abuse may emerge before the law clearly addresses the specific method used. However, this does not mean that a completely new criminal offence must be created every time technology changes. In some situations, existing legal provisions may already apply.

The greater challenge is often the effective implementation of existing laws. Police officers and investigators need proper training in cybercrime investigation, digital evidence, online identification, and electronic communication.

Women should also have simple and accessible ways to report online abuse. Complaints should

be dealt with promptly, and victims should receive appropriate assistance throughout the legal process.

VII. IMPACT OF DIGITAL VIOLENCE ON WOMEN

Digital violence can have serious effects on a woman's personal, social, educational, and professional life.

For example, if a private photograph is shared online without consent, the victim may face embarrassment, threats, blackmail, social criticism, or damage to her reputation. The consequences may continue even after the original post has been removed because copies may have already been circulated.

Online stalking can also create a constant feeling of insecurity. A woman may feel that the offender can reach her at any time through her phone, email, or social media accounts, even when she is physically at home.

Such experiences may affect a woman's education, employment, relationships, and participation in social life. Some victims may stop using social media or avoid digital communication because they fear further harassment.

Therefore, digital violence should be treated as a serious form of harm. The main difference is the method through which the abuse is carried out, not necessarily the seriousness of its consequences.

VIII. RESEARCH METHODOLOGY

This study follows a **doctrinal method of legal research**. It examines legislation, judicial decisions, legal literature, government materials, and other relevant legal sources.

The study mainly focuses on the BNS, the IT Act, and the BSA to understand how Indian law responds to violence against women in the digital environment.

It also examines practical problems relating to identifying offenders, collecting and preserving electronic evidence, determining jurisdiction, conducting investigations, and enforcing the law.

The purpose of this research is to identify the areas in which the existing legal framework

provides protection and the areas where further legal or institutional improvement may be necessary.

IX. MAIN ARGUMENT OF THE STUDY

The main argument of this study is that India has several laws that can protect women from different forms of violence, including certain types of digital abuse. However, technological development has created challenges that cannot always be effectively addressed through traditional methods of criminal investigation.

The effectiveness of legal protection depends on several factors. These include the ability of investigators to identify offenders, the proper collection and preservation of digital evidence, access to technical expertise, cooperation with online platforms, and the ability of courts to assess electronic evidence.

There is therefore a need to strengthen cyber investigation facilities and provide regular training to police officers, investigators, prosecutors, and other members of the criminal justice system.

Women should also be informed about their legal rights and the available mechanisms for reporting online abuse. At the same time, the privacy and dignity of victims should be protected during investigation and court proceedings.

The broader aim should be to create a criminal justice system that is capable of responding to both traditional violence and new forms of technology-based abuse.

X. SUGGESTIONS

The following measures can help improve the protection of women against digital violence:

a) Specialized Training

Police officers and investigators should receive regular training in cybercrime investigation, digital forensics, electronic evidence, and online identification techniques.

b) Better Cyber Forensic Facilities

Cyber forensic laboratories and technical resources should be strengthened so that digital

evidence can be examined quickly and accurately.

c) Proper Preservation of Digital Evidence

Evidence such as messages, photographs, videos, emails, and social media records should be preserved at an early stage so that important material is not lost or altered.

d) Easy Reporting Mechanisms

Women should have simple and accessible methods for reporting online stalking, harassment, threats, blackmail, and privacy violations. Complaints should be handled promptly and sensitively.

e) Cooperation Between Authorities and Digital Platforms

Law-enforcement agencies should have effective procedures for obtaining relevant information from online platforms in accordance with law and due process.

f) Legal Awareness

Women should be made aware of their legal rights and the remedies available when they face online abuse. Public awareness can also help victims understand how to preserve important digital evidence.

g) Protection of Victims' Privacy

The investigation and prosecution of digital offences should be carried out in a manner that protects the identity, dignity, and personal information of victims.

h) Regular Review of Laws

Criminal laws and investigative procedures should be reviewed periodically because technology and methods of online abuse continue to change.

XII. CONCLUSION

Violence against women is no longer limited to physical places. Digital technology has created new ways in which women can be threatened, stalked, harassed, sexually exploited,

impersonated, or subjected to violations of privacy.

India has developed a legal framework that can address many forms of such conduct. The BNS recognises digital monitoring as part of stalking, the IT Act deals with several forms of cyber-related conduct, and the BSA provides an important framework for dealing with electronic and digital evidence.⁹

However, having laws on paper is not enough. Their effectiveness depends on proper investigation and enforcement. Difficulties such as anonymous offenders, deletion of digital evidence, cross-border information, jurisdictional problems, and lack of technical expertise can make it difficult for victims to obtain timely justice.

The solution therefore requires more than simply creating additional offences. India needs a coordinated system involving effective laws, trained investigators, modern forensic facilities, proper evidence-preservation procedures, accessible complaint mechanisms, and strong protection for victims.

Ultimately, technological development should not leave women less protected. Their rights to **safety, dignity, privacy, and access to justice** should be protected both in physical spaces and in the digital environment.

Endnotes:

1. The Bharatiya Nyaya Sanhita, 2023, 78 (stalking), including monitoring of a woman's internet, email, or other electronic communication. India Code, The Bharatiya Nyaya Sanhita, 2023. I India Code
2. The Information Technology Act, 2000, 66C, 66D, 66E, 67 and 67A. India Code, The Information Technology Act, 2000.
3. The Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023. Ministry of Home Affairs, Government of India, *New Criminal Laws*.
4. The Bharatiya Nyaya Sanhita, 2023, 78. The provision expressly includes monitoring the use of internet, email, or another form of electronic communication as a form of stalking, subject to the statutory exceptions. I India Code
5. The Information Technology Act, 2000, 66E, *Punishment for violation of privacy*. The provision concerns the intentional or knowing capture, publication, or transmission of an image of a private area without consent in circumstances violating privacy.
6. The Information Technology Act, 2000, 67 and 67A, concerning publication or transmission of obscene material and material containing sexually explicit acts in electronic form.
7. The Bharatiya Sakshya Adhiniyam, 2023, 61–63. Section 61 recognises electronic or digital records, while sections 62 and 63 provide rules concerning proof and admissibility of electronic records.
8. The Bharatiya Sakshya Adhiniyam, 2023, 61–63. The Act came into force on 1 July 2024.
9. The Bharatiya Nyaya Sanhita, 2023, 78; the Information Technology Act, 2000, 66E, 67 and 67A; and the Bharatiya Sakshya Adhiniyam, 2023, 61–63.

Primary Legal Sources

- *The Bharatiya Nyaya Sanhita, 2023*, Act No. 45 of 2023.
- *The Information Technology Act, 2000*, Act No. 21 of 2000.
- *The Bharatiya Sakshya Adhiniyam, 2023*, Act No. 47 of 2023.