PSYCHOLOGICAL VICTIMISATION OF WOMEN THROUGH CYBERCRIME: A VICTIMOLOGICAL ANALYSIS

Kaviya R, LLM, Department of Criminal Law and Criminal Justice Administration, School of Excellence in Law, The Tamil Nadu, Dr. Ambedkar Law University, Chennai, Tamil Nadu, India

ABSTRACT

The rapid development of the internet, social media and digital communication has created new forms of victimisation against women. Cyberstalking, cyber harassment, online sexual harassment, non-consensual sharing of intimate images, sextortion, morphing, deepfakes, doxxing and online threats can cause serious psychological harm. Unlike many traditional offences, cyber victimisation can continue after the original incident because digital content can be copied, shared and accessed repeatedly. This may result in fear, anxiety, humiliation, shame, emotional distress, loss of self-esteem and social isolation. This article examines the psychological victimisation of women through a victimological perspective. It focuses on victim vulnerability, victim-offender relationships, repeat victimisation, victim-blaming, stigma, secondary victimisation and underreporting. It further examines the Indian legal framework, including the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023 and Information Technology Rules. The article identifies gaps relating to psychological support, emerging technologies, digital evidence, content circulation and victim rehabilitation. It proposes a victim-centred approach based on prevention, protection, investigation, justice and psychological recovery.

Keywords: Cybercrime; Psychological Victimisation; Women; Victimology; Cyberstalking; Underreporting.

I. INTRODUCTION

The rapid growth of the internet and social media has changed the way people communicate and interact. At the same time, digital technology has created new opportunities for criminal activities against women. Cyberstalking, cyber harassment, online sexual harassment, non-consensual sharing of intimate images, sextortion, morphing, deepfakes and online threats are some of the forms through which women may experience cyber victimisation.[1]

Cybercrime against women does not cause only legal or financial harm. It can also affect their psychological well-being. Fear, anxiety, humiliation, shame, emotional distress, loss of confidence and social isolation may follow an online incident. The impact may become more serious when harmful content continues to circulate on different digital platforms.

Victimology provides an important way of understanding this problem because it focuses on the victim and the experience of victimisation. It considers factors such as vulnerability, victim-offender relationships, repeat victimisation, victim-blaming, stigma and secondary victimisation.

India has several legal provisions dealing with cyber offences and offences against women. The Information Technology Act, 2000 and the new criminal laws, namely the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, provide different forms of legal protection and procedure. However, effective protection requires more than punishment of offenders. The psychological needs, privacy, dignity, safety and rehabilitation of victims must also receive attention.[2]

This article therefore examines cybercrime against women from a victimological perspective, with particular emphasis on psychological victimisation, underreporting and the need for a victim-centred legal and institutional response.

II. CONCEPT OF PSYCHOLOGICAL VICTIMISATION IN CYBERSPACE

Psychological victimisation refers to the mental and emotional harm experienced by a person because of criminal or abusive conduct. In cyberspace, psychological victimisation may occur

[1] Sherin Farhana Ev, "Cyber Crimes and the Victimisation of Women," *International Journal of Law Management & Humanities*, Vol. 5, Issue 1, 2022.
[2] Vishakha Tyagi, "Victimization of Women in Cybercrime: An International Perspective," *International Journal of Law Management & Humanities*, Vol. 6, Issue 6, 2023.

when a person is repeatedly threatened, harassed, stalked, humiliated, sexually abused or exposed through digital platforms.

The psychological impact of cybercrime may include fear, anxiety, stress, shame, anger, sadness, helplessness, loss of confidence and a feeling of insecurity.[3] The victim may also become afraid of using social media or other digital services because of the possibility of further abuse.

Women may be particularly affected by cybercrimes involving sexuality, appearance, relationships and private information. For example, an intimate photograph shared without consent may reach people known to the victim, while a manipulated sexual image may be circulated among strangers. The victim may therefore fear both public humiliation and personal consequences.

An important feature of cyber victimisation is the continuing nature of digital content. A physical act may end after the incident, but online content can be copied, downloaded, forwarded and uploaded again. This can create a continuing fear of exposure and repeat victimisation.

Psychological victimisation should therefore be understood as an important part of the total harm caused by cybercrime. The legal response should not focus only on identifying the offender and removing the content; it should also consider the victim's emotional safety and recovery.[4]

III. CYBERCRIMES RESULTING IN PSYCHOLOGICAL VICTIMISATION OF WOMEN

Cybercrime against women can take several forms. Different forms of cybercrime may produce different types and levels of psychological harm.

1. Cyberstalking

Cyberstalking involves repeated unwanted digital contact, monitoring or following of a person.

[3] Prerana Bhaskar Mahajan & P. Paul Ramesh, "Humanizing Cybersecurity: Addressing the Psychological Impact of Cybercrime," *International Journal of Indian Psychology*, Vol. 13, Issue 3, 2025.
[4] Vishakha Tyagi, "Victimization of Women in Cybercrime: An International Perspective," *International Journal of Law Management & Humanities*, Vol. 6, Issue 6, 2023.

An offender may repeatedly send messages, monitor social media activity, create fake accounts or attempt to track the victim's online activities.

The continuous nature of cyberstalking can make the victim feel that she is being watched. Even when there is no immediate physical contact, the victim may fear that the offender knows her movements, relationships or personal information. This may result in anxiety and fear.

Section 78 of the Bharatiya Nyaya Sanhita, 2023 deals with stalking and includes monitoring the use by a woman of the internet, email or other electronic communication.[5]

2. Cyber Harassment

Cyber harassment includes repeated abusive, insulting, threatening or offensive communication through social media, email, messaging applications or other digital platforms.

Harassment can affect the victim's emotional well-being, particularly when it occurs repeatedly or is accompanied by threats. Anonymous accounts can make the victim uncertain about the identity of the offender and may increase feelings of insecurity.

3. Online Sexual Harassment

Women may receive unwanted sexual messages, sexually explicit material, offensive comments or sexual threats through digital platforms. Such conduct may cause embarrassment, humiliation and fear.

Depending upon the facts, provisions of the Information Technology Act and the Bharatiya Nyaya Sanhita may become relevant. Section 75 of the BNS deals with sexual harassment, while the IT Act contains provisions relating to sexually explicit material in electronic form.

4. Non-Consensual Sharing of Intimate Images

The non-consensual sharing of intimate images is one of the serious forms of online victimisation. The offender may publish or forward private images to friends, family members, colleagues or the public.

[5] The Bharatiya Nyaya Sanhita, 2023, s. 78.

The psychological impact may be severe because the victim may lose control over who can see the material. Even after removal from one platform, copies may remain available elsewhere.

5. Sextortion

Sextortion generally involves the use of intimate images, videos or information to threaten or pressure a person to provide money, further images, sexual acts or other demands.

The victim may experience continuous fear because the offender can threaten to publish the material at any time. This can create a strong feeling of helplessness.

6. Morphing and Deepfakes

Morphing involves manipulation of an existing photograph or image. Deepfake technology can create realistic artificial images, videos or audio using digital tools.

Sexualised deepfakes involving women may damage dignity, privacy and reputation even when the woman never created or consented to the material. The increasing availability of artificial intelligence has made this issue particularly important.

The Government has identified deepfakes and synthetic media as emerging concerns and has referred to existing provisions of the IT Act, including Sections 66C, 66D, 66E, 67 and 67A, as relevant legal provisions depending on the conduct involved.[6]

7. Doxxing and Privacy Invasion

Doxxing involves publishing personal information such as telephone numbers, addresses, workplace details or other private information without permission.

The victim may fear that the online disclosure will lead to physical harassment or stalking. Thus, online privacy invasion can create fear beyond the digital environment.

Section 66E of the IT Act specifically addresses violation of privacy in relation to certain private images.

[6] Ministry of Electronics and Information Technology, Government of India, materials on legal safeguards concerning AI-generated deepfakes.

8. Online Threats and Intimidation

Online threats may relate to physical harm, sexual violence, reputational damage or publication of private information. Such threats may amount to criminal intimidation depending upon the facts.

Section 351 of the BNS deals with criminal intimidation. When threats are made through digital communication, the electronic messages, screenshots and other digital records may become relevant evidence. Cybercrime against women therefore includes a wide range of conduct. These offences may overlap, and one incident may involve several forms of victimisation.

IV. PSYCHOLOGICAL CONSEQUENCES OF CYBERCRIME AGAINST WOMEN

The psychological consequences of cybercrime depend upon the nature, seriousness and duration of the victimisation. The identity of the offender and the extent of circulation of harmful material may also influence the victim's experience.

1. Fear and Anxiety

Threats, stalking and repeated harassment can create a continuing feeling of fear. The victim may become anxious whenever she receives a message, notification or unknown call. Where the offender is known to the victim, the fear may become stronger because the offender may possess information about her family, workplace or personal relationships.

2. Humiliation and Shame

Sexualised online content can cause intense feelings of embarrassment and humiliation. A victim may fear that family members, friends, colleagues or employers will see the material. This can lead to withdrawal from social activities and reluctance to seek help.

3. Loss of Self-Esteem

Repeated insults, sexual comments, threats or publication of manipulated images may affect the victim's confidence. The victim may begin to question her appearance, identity or social relationships. The emotional harm may be particularly serious when the abuse continues for a long period.

4. Emotional Distress

Victims may experience sadness, anger, frustration, helplessness and emotional exhaustion. The victim may spend considerable time trying to remove content, block accounts or identify the offender. The effort required to manage the incident may itself become a source of stress.

5. Social Isolation

Some women may stop using social media or reduce contact with others because they fear further harassment. In serious cases, they may avoid educational institutions, workplaces or social gatherings. Thus, cybercrime may affect not only digital life but also education, employment and personal relationships.

6. Fear of Repeat Victimisation

A major feature of cybercrime is the possibility of repetition. The offender may create a new account, repost content or contact the victim through another platform. The victim may therefore continue to feel unsafe even after making a complaint.

7. Loss of Digital Trust

A victim may lose confidence in digital platforms, online communication and even personal relationships. This may affect her willingness to use technology for education, employment or social communication.

Psychological harm therefore forms an important part of the overall consequences of cybercrime. A criminal justice response that considers only the offence and offender may fail to address the full experience of the victim.[7]

V. VICTIMOLOGICAL ANALYSIS OF WOMEN'S CYBER VICTIMISATION

Victimology focuses on victims, victimisation and the relationship between victims, offenders and the criminal justice system. Applying a victimological approach to cybercrime helps to understand the reasons why psychological harm may continue after the offence.

[7] Prerana Bhaskar Mahajan & P. Paul Ramesh, "Humanizing Cybersecurity: Addressing the Psychological Impact of Cybercrime," *International Journal of Indian Psychology*, Vol. 13, Issue 3, 2025.

1. Victim Vulnerability

Women may face cyber victimisation because offenders misuse publicly available information, personal photographs, social-media accounts or private communications. However, vulnerability must not be confused with responsibility. The fact that a woman uses social media, shares photographs or communicates online does not justify criminal conduct against her. The responsibility for the offence remains with the offender.

2. Victim-Offender Relationship

The offender may be a stranger, acquaintance, former partner, friend or another known person. In cases involving former intimate partners, the offender may possess private photographs, messages or personal information. The existing relationship may therefore be used as a means of control, intimidation or humiliation.

3. Repeat Victimisation

Digital technology makes repeated victimisation easier. An offender can use multiple accounts, platforms and communication methods. The victim may therefore experience several incidents arising from the same original event. Repeat victimisation increases fear and can reduce confidence in the effectiveness of protective measures.

4. Victim-Blaming

Victim-blaming occurs when attention is shifted from the offender's conduct to the behaviour of the victim. For example, a victim of non-consensual image sharing may be questioned about why she created or shared the photograph. Such an approach can discourage reporting and create additional psychological harm. The central legal question should be whether the content was used or distributed without consent and whether the conduct violated applicable law.

5. Stigma

Social attitudes may make it difficult for women to disclose sexual or humiliating cyber victimisation. Fear of being judged by family members, friends or society may discourage victims from seeking help. Stigma can therefore contribute directly to underreporting.

6. Secondary Victimisation

Secondary victimisation occurs when the victim suffers additional harm after the original offence through insensitive treatment by institutions or society. A victim may be required to repeatedly explain humiliating events, may face unnecessary questioning or may feel that her complaint is not taken seriously. Police, investigators, lawyers and courts therefore have an important role in ensuring respectful and confidential treatment.

7. Underreporting

The psychological effects of shame, fear, stigma and uncertainty can prevent victims from reporting. Underreporting also makes it difficult to understand the full extent of cyber victimisation. A victimological approach therefore requires attention to the complete experience of the victim, from the initial offence to reporting, investigation and recovery.

VI. UNDERREPORTING OF CYBERCRIME AGAINST WOMEN

Underreporting is an important problem in cybercrime against women. The decision not to report may result from several personal, social and institutional factors. First, victims may feel ashamed or embarrassed, particularly where the incident involves sexual content or intimate images. Secondly, they may fear that reporting will make the incident known to family members, friends or colleagues. Thirdly, victims may fear retaliation. An offender may threaten to publish additional material or harm the victim if she makes a complaint. Fourthly, lack of awareness about available remedies can prevent reporting. A victim may not know whether an incident is a criminal offence, how to preserve digital evidence or where to complain. Fifthly, previous negative experiences or fear of insensitive treatment may reduce trust in institutions.

Underreporting has consequences for both the victim and the criminal justice system. The victim may remain without protection, while offenders may continue their conduct without intervention.

India's National Cyber Crime Reporting Portal provides an online mechanism for reporting cybercrime and includes facilities for complaints relating to women and children. The national cybercrime helpline **1930** also provides a mechanism for cybercrime-related assistance.

However, reporting mechanisms must be accompanied by confidentiality, legal guidance and

psychological support. A woman should feel safe while making a complaint.

VII. INDIAN LEGAL FRAMEWORK FOR PROTECTION OF WOMEN FROM CYBER VICTIMISATION

Indian law addresses cyber victimisation through several statutes rather than through one comprehensive law.

1. Information Technology Act, 2000

The Information Technology Act, 2000 is the principal legislation dealing specifically with various forms of cyber conduct. Section 66C deals with identity theft and Section 66D deals with cheating by personation using a computer resource. Section 66E deals with violation of privacy. Sections 67 and 67A address the publication or transmission of obscene and sexually explicit material in electronic form. These provisions may become relevant in cases involving sexualised digital content. Section 67C concerns preservation and retention of information by intermediaries. Digital evidence and preservation are particularly important in cybercrime cases because online content may be deleted or modified quickly. The Act therefore provides important criminal provisions, but its provisions must often operate together with other laws depending upon the facts.

2. Bharatiya Nyaya Sanhita, 2023

The BNS contains several provisions relevant to women and conduct occurring through digital means. Section 75 deals with sexual harassment. Section 78 deals with stalking, including monitoring the use by a woman of the internet, email or other electronic communication. Section 79 addresses words, gestures or acts intended to insult the modesty of a woman. Section 351 deals with criminal intimidation and Section 356 deals with defamation. These provisions may become relevant where cyber conduct includes threats or reputational harm. The application of these provisions depends upon the facts and evidence in each case.

3. Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS provides procedural protections and victim compensation mechanisms. Section 396 provides for a victim compensation scheme. It permits compensation to victims who have suffered loss or injury as a result of crime and require rehabilitation. The provision also

contemplates situations where the offender has not been traced or identified. This is significant because cybercrime can cause psychological and social consequences even where the offender cannot immediately be identified. However, compensation should be understood as one part of victim support. Psychological counselling, legal assistance, privacy protection and rehabilitation are also necessary.

4. Bharatiya Sakshya Adhiniyam, 2023

Digital evidence is central to cybercrime cases. Screenshots, emails, messages, videos, social-media records and other electronic material may be important for establishing the offence. Section 61 of the BSA recognises electronic or digital records, subject to the provisions of the Act. Section 63 deals with admissibility of electronic records and sets out the relevant conditions. The preservation and proper handling of digital evidence are therefore important for both investigation and trial.

5. Information Technology Rules

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 establish obligations concerning intermediaries and grievance redressal. The Rules are relevant to victims because online platforms may be the place where unlawful content is uploaded, circulated or reported. Effective grievance mechanisms can assist in limiting further circulation of harmful content. The regulatory framework concerning synthetic and AI-generated content has also developed further, reflecting the increasing importance of deepfakes and other forms of synthetic media.

6. National Cyber Crime Reporting Portal

The National Cyber Crime Reporting Portal provides an online mechanism through which cybercrime complaints can be submitted. It is particularly relevant to women and children. The portal is an important reporting mechanism, but it cannot replace the need for effective police investigation, evidence preservation and victim support.

Therefore, the Indian legal framework contains significant protections, but the effectiveness of those protections depends upon coordination between law enforcement, courts, intermediaries and victim-support institutions.

VIII. GAPS IN THE EXISTING LEGAL FRAMEWORK

The Indian legal framework provides several remedies, but certain practical and legal gaps remain.

1. Fragmented Legal Framework

Cyber victimisation may involve provisions under more than one statute. A single incident may involve privacy violation, sexual harassment, intimidation, publication of obscene material and other offences. This may make the legal process difficult for victims who are unfamiliar with the criminal justice system.

2. Limited Recognition of Psychological Harm

Criminal law generally focuses on identifying the offence, collecting evidence and punishing the offender. Psychological consequences are not always given sufficient attention during investigation and rehabilitation. A victim may require counselling even where the criminal case is still pending.

3. Deepfakes and Artificial Intelligence

AI-generated sexual images and videos create new challenges. A victim may be represented in content that she never created and never consented to. Attribution can also be difficult because offenders may use anonymous accounts, foreign platforms or automated tools.

The Government has acknowledged deepfake-related risks and, during 2026, described the existing legal and regulatory framework as addressing various aspects of AI-generated deepfakes.[8] However, the development of technology requires continuing review of the adequacy of existing legal mechanisms.

4. Rapid Circulation of Content

Digital content can spread rapidly through multiple platforms. Removing one copy does not necessarily guarantee that all copies have disappeared. This creates a continuing problem for

[8] Ministry of Electronics and Information Technology, Government of India, "Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes," 2026.

victims and can extend psychological harm.

5. Anonymity

Offenders may use fake identities, temporary accounts or other methods to conceal their identity. This can create difficulties in attribution and investigation.

6. Cross-Border Nature

A victim in India may be targeted by an offender located in another country, or harmful content may be hosted on a foreign platform. Cross-border investigations can involve jurisdictional and procedural difficulties.

7. Digital Evidence

Evidence may be deleted, altered or lost. Victims may also unintentionally modify evidence by deleting messages or accounts. Awareness regarding preservation of screenshots, URLs, account details, messages and other relevant records is therefore important.

8. Secondary Victimisation

Even where legal remedies are available, insensitive questioning, unnecessary disclosure of private material or victim-blaming can cause additional harm. Victim protection must therefore form part of the investigation process.

IX. VICTIM-CENTRED LEGAL AND INSTITUTIONAL APPROACH

A victim-centred approach means that the victim's safety, dignity, privacy and psychological well-being are considered throughout the justice process.

Such an approach can be understood through five stages.

1. Prevention

Prevention includes digital literacy, privacy awareness and education about safe online behaviour. Women should be informed about reporting mechanisms and methods of preserving digital evidence.

2. Protection

Once cyber victimisation occurs, immediate steps should be taken to prevent further harm. This may include blocking or reporting accounts, protecting personal information and seeking removal of unlawful content through appropriate channels.

3. Investigation

Cybercrime investigators should have appropriate technical knowledge and should collect digital evidence without unnecessarily exposing the victim's private information. The victim should not be treated as responsible for the offender's conduct.

4. Justice

Victims should have meaningful access to legal remedies and should be informed about the progress of their complaint where appropriate. Investigation should be conducted in a manner that respects privacy and dignity.

5. Psychological Recovery

Recovery should not be ignored after investigation. Victims may require counselling, legal assistance and social support.

This five-stage approach recognises that justice is not limited to punishment. Protection and recovery are also important components of a victim-centred response.

X. SUGGESTIONS

1. Establish Specialised Cyber Victim Support Units

Specialised units may be established within cybercrime structures to provide women victims with legal guidance, assistance in preserving evidence and access to counselling.

2. Provide Gender-Sensitive Training

Police officers, investigators and other officials should receive training on the psychological consequences of cybercrime against women.

The training should emphasise confidentiality, dignity and avoidance of victim-blaming.

3. Strengthen Psychological Support

Victims experiencing serious emotional distress should have access to professional psychological counselling. Such support should be treated as part of victim assistance rather than as an optional service.

4. Improve Content-Removal Mechanisms

Where unlawful intimate or sexual content is circulated online, reporting and grievance mechanisms should function efficiently to reduce further circulation.

5. Address Deepfake Victimisation

The legal and institutional framework should continue to develop mechanisms for identifying, reporting and responding to harmful AI-generated content, particularly sexually explicit deepfakes involving women.

6. Strengthen Victim Compensation

Compensation mechanisms should recognise that victimisation may involve financial, psychological and social consequences. Access to compensation should be made simple and accessible. Section 396 of the BNSS provides a statutory framework for victim compensation and rehabilitation.[9]

7. Protect Victim Confidentiality

Personal information, intimate images and sensitive details of victims should be handled carefully during investigation and judicial proceedings.

8. Improve Awareness of Reporting Mechanisms

Women should be informed about the National Cyber Crime Reporting Portal, the 1930 cybercrime helpline and other available legal mechanisms.

[9] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 396.

9. Preserve Digital Evidence

Awareness programmes should explain the importance of preserving relevant messages, screenshots, URLs, emails, account details and other digital records.

10. Prevent Secondary Victimisation

The justice system should avoid unnecessary repetition of humiliating experiences and should ensure respectful communication with victims.

11. Improve Institutional Coordination

Police, cybercrime units, prosecutors, courts, intermediaries, legal services institutions and mental-health professionals should coordinate when dealing with serious cyber victimisation.

12. Promote Digital Literacy

Digital literacy should include not only technical skills but also awareness about consent, privacy, cyber safety, reporting and legal remedies.

XI. CONCLUSION

Cybercrime against women is a growing area of concern because its consequences may extend beyond the immediate digital incident. Cyberstalking, harassment, sexual abuse, non-consensual intimate-image sharing, sextortion, morphing, deepfakes, doxxing and online threats can cause fear, anxiety, humiliation, emotional distress and loss of confidence.

A victimological approach provides a broader understanding of this problem. It focuses on the victim's experience and considers vulnerability, victim-offender relationships, repeat victimisation, victim-blaming, stigma, secondary victimisation and underreporting. This approach also shows why the response to cybercrime should not end with identification and punishment of the offender.

India has several legal provisions that can be applied to cyber victimisation. The Information Technology Act, 2000 addresses identity theft, impersonation, privacy violations and certain forms of obscene and sexually explicit electronic content. The Bharatiya Nyaya Sanhita, 2023 contains provisions relevant to stalking, sexual harassment, intimidation and other offences.

The Bharatiya Nagarik Suraksha Sanhita, 2023 provides a framework for victim compensation, while the Bharatiya Sakshya Adhiniyam, 2023 provides for electronic and digital records as evidence. The Information Technology Rules and the National Cyber Crime Reporting Portal further contribute to the regulatory and reporting framework.

At the same time, the existence of legal provisions does not automatically ensure effective recovery for victims. Psychological harm, repeat victimisation, rapid circulation of content, anonymity, deepfakes, cross-border offending and secondary victimisation require continuing legal and institutional attention.

The appropriate response should therefore be **victim-centred rather than limited to an offence-centred approach**. Prevention, protection, investigation, justice and psychological recovery should operate together. Women who experience cybercrime should be able to report the offence without fear, preserve their dignity and privacy, receive appropriate legal and psychological assistance and obtain effective remedies.

Ultimately, addressing psychological victimisation requires recognition that cybercrime can affect not only a woman's digital identity but also her dignity, emotional security, social relationships and everyday life. A comprehensive victim-centred framework can help ensure that the response to cybercrime protects both the **legal rights and psychological well-being of women victims**.

REFERENCES

Legislation

1. Information Technology Act, 2000.
2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
3. Bharatiya Nyaya Sanhita, 2023.
4. Bharatiya Nagarik Suraksha Sanhita, 2023.
5. Bharatiya Sakshya Adhiniyam, 2023.

Articles and Books

6. Sherin Farhana Ev, "Cyber Crimes and the Victimisation of Women," *International Journal of Law Management & Humanities*, Vol. 5, Issue 1, 2022.
7. Vishakha Tyagi, "Victimization of Women in Cybercrime: An International Perspective," *International Journal of Law Management & Humanities*, Vol. 6, Issue 6, 2023.
8. Prerana Bhaskar Mahajan & P. Paul Ramesh, "Humanizing Cybersecurity: Addressing the Psychological Impact of Cybercrime," *International Journal of Indian Psychology*, Vol. 13, Issue 3, 2025.
9. Sandra Walklate, *Victimology: The Victim and the Criminal Justice Process*.
10. Andrew Karmen, *Crime Victims: An Introduction to Victimology*.

Institutional Sources

11. Ministry of Home Affairs, Government of India, materials relating to the new criminal laws.
12. Ministry of Electronics and Information Technology, Government of India, materials relating to intermediary regulation and AI-generated content.
13. National Cyber Crime Reporting Portal, Government of India.
14. National Crime Records Bureau, Government of India.
15. United Nations Office on Drugs and Crime, materials on cybercrime and victimisation.
16. UN Women, materials on violence against women in digital spaces.