INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

CYBER CRIME AGAINST WOMEN

AUTHORED BY - KIRANDEEP KAUR[1] DR. SWAPANPREET KAUR[2]

Abstract

The rapid growth of digital technology and internet accessibility has significantly increased the incidence of cybercrime across the world, particularly crimes targeting women. Cybercrime against women includes offenses such as cyberstalking, online harassment, identity theft, cyberbullying, revenge pornography, morphing, sextortion, and defamation through social media and digital platforms. In India, the widespread use of smartphones and social networking applications has created new opportunities for offenders to exploit women psychologically, socially, and financially. Despite the existence of legal provisions under the Information Technology Act, 2000, Bharatiya Nyaya Sanhita (BNS), and other cyber laws, many cases remain unreported due to fear of social stigma, lack of awareness, and inadequate cyber law enforcement mechanisms.

This study examines the nature, causes, and impact of cybercrime against women and analyzes the effectiveness of existing legal frameworks and government initiatives in addressing such offenses. The paper also highlights the psychological trauma, reputational damage, and social insecurity experienced by victims. Furthermore, it emphasizes the importance of cyber awareness, digital literacy, strict implementation of laws, and cooperation between law enforcement agencies, educational institutions, and society to ensure women's safety in cyberspace. The study concludes that strengthening cyber laws, improving reporting mechanisms, and promoting awareness programs are essential steps toward combating cybercrime against women and creating a safer digital environment.

[1] Student of LL.M, Student ID: 25072001097, University School of Law, Rayat Bahra University, Punjab, India.
[2] Head of Department, University School of Law, Rayat Bahra University, Punjab, India.

Keywords

Cybercrime, Women Safety, Cyberstalking, Online Harassment, Cyberbullying, Revenge Pornography, Information Technology Act, Digital Violence, Cyber Law, Social Media Abuse, Sextortion, Women Empowerment.

Introduction

In the contemporary digital era, the internet has become an essential part of everyday life, transforming communication, education, business, entertainment, and social interaction. The rapid advancement of information technology and the widespread use of smartphones and social media platforms have created numerous opportunities for individuals across the globe. However, along with these technological benefits, the rise in cybercrime has emerged as a serious challenge to society. Among the various forms of cybercrime, offenses targeting women have become increasingly common and alarming.

Cybercrime against women refers to criminal activities carried out through digital technologies, computers, mobile devices, or online platforms with the intention of harassing, threatening, exploiting, or harming women psychologically, socially, financially, or emotionally. These crimes include cyberstalking, online harassment, cyberbullying, identity theft, email spoofing, morphing of images, revenge pornography, sextortion, and defamation through social media. The anonymity provided by the internet often encourages offenders to commit such crimes without fear of immediate identification or punishment.

In India, the rapid growth of internet users and digital communication platforms has increased women's participation in cyberspace, but it has also exposed them to new forms of exploitation and abuse. Social networking websites, messaging applications, and online forums are frequently misused to target women through abusive messages, fake profiles, blackmail, and unauthorized sharing of personal information or intimate images. Such acts not only violate the privacy and dignity of women but also cause severe emotional distress, depression, fear, and social insecurity. Although the Government of India has introduced several legal provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita (BNS), and other cyber laws to address cyber

offenses, the increasing number of cases indicates that legal and enforcement mechanisms still face significant challenges. Lack of awareness, underreporting of crimes, social stigma, inadequate cyber literacy, and delays in investigation often prevent victims from obtaining justice.

This research paper aims to examine the various forms of cybercrime against women, analyze their causes and impact, evaluate the effectiveness of existing legal frameworks, and suggest preventive measures to enhance women's safety in the digital environment. The study also emphasizes the importance of cyber awareness, education, and collective social responsibility in combating cybercrime and promoting a secure cyberspace for women.

Research Problem and Objectives

Research Problem

The rapid expansion of digital technology and internet usage has led to a significant increase in cybercrimes targeting women. Despite the implementation of cyber laws and legal safeguards in India, women continue to face various forms of online abuse such as cyberstalking, cyberbullying, identity theft, online harassment, revenge pornography, morphing, and sextortion. Many victims hesitate to report such crimes due to fear of social stigma, lack of awareness, privacy concerns, and limited trust in law enforcement agencies. Furthermore, the anonymity of cyberspace and the evolving nature of technology make detection, investigation, and prosecution of offenders difficult.

The increasing incidents of cybercrime against women raise serious concerns regarding women's safety, privacy, dignity, and mental well-being in the digital environment. Therefore, there is a need to critically examine the nature and impact of cybercrime against women, evaluate the effectiveness of existing legal frameworks, and identify measures for prevention and protection in cyberspace.

Research Objectives

The main objectives of this research study are:

- To understand the concept and various forms of cybercrime against women.
- To examine the major causes and factors contributing to cybercrime against women.
- To analyze the social, psychological, and emotional impact of cybercrime on women

victims.

- To study the legal provisions and cyber laws related to the protection of women in cyberspace, particularly under the Information Technology Act, 2000 and Bharatiya Nyaya Sanhita (BNS).
- To evaluate the effectiveness of law enforcement agencies and cybercrime reporting mechanisms in addressing crimes against women.
- To identify the challenges faced by victims in reporting and seeking justice for cyber offenses.
- To suggest preventive measures and policy recommendations for ensuring women's safety and security in the digital environment.

Research Methodology

The research on "Cyber Crime Against Women in India" is based on a descriptive and analytical design using a mixed-method approach. Both primary and secondary data have been used to ensure a comprehensive understanding of the topic. Primary data was collected through questionnaires, online surveys, and interviews from women internet users, students, working women, and cyber experts. Secondary data was gathered from books, journals, newspapers, government reports, NCRB statistics, and legal documents such as the Information Technology Act, 2000 and other cyber laws. A random and purposive sampling technique was used to select respondents for the study.

The study is primarily based on secondary sources of data. Relevant information has been collected from books, research journals, articles, government reports, NCRB statistics, case laws, legal databases, and online academic sources relating to cyber crimes against women. Statutory provisions and judicial decisions have been critically analysed to understand the scope and implementation of cyber laws in India. The research adopts a doctrinal method to interpret legal provisions and an analytical approach to identify challenges and suggest preventive measures for ensuring the safety and protection of women in cyberspace.

Cyber-crime against women in India

Cyber crime against women in India has increased rapidly with the growth of internet usage and social media platforms. Women are often targeted through offences such as cyber stalking, online harassment, cyber bullying, identity theft, revenge pornography, and morphing of photographs. These crimes violate the privacy, dignity, and security of women and cause serious psychological and social harm. Many victims hesitate to report such offences due to fear of social stigma and lack of awareness. The Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 provide legal protection against cyber offences targeting women. However, challenges such as low cyber awareness, delayed investigation, and misuse of technology continue to hinder effective enforcement. The rise of artificial intelligence and deepfake technology has further increased the risk of online exploitation of women. Therefore, stronger cyber laws, digital literacy, and effective law enforcement are essential to ensure the safety of women in cyberspace.

Meaning of cyber crimes

Cyber crime refers to any unlawful or criminal activity committed using computers, digital devices, computer networks, or the internet. It involves the misuse of technology to steal data, invade privacy, commit fraud, spread harmful content, or cause damage to individuals, organizations, or governments. Cyber crimes may be committed against a computer system, such as hacking and malware attacks, or through a computer system, such as online fraud, cyber stalking, identity theft, and cyber bullying. With the increasing use of digital technology and internet services, cyber crime has become a major threat affecting security, privacy, and social well-being across the world.

Types of cyber crimes against women

1. Cyber Stalking

Cyber stalking refers to the repeated use of the internet, social media, emails, or messaging applications to harass, monitor, threaten, or intimidate a woman. The offender may continuously send unwanted messages, track online activities, monitor location, or attempt to establish unwanted communication. In many cases, cyber stalkers create fear and emotional distress in the minds of victims. Such acts may also extend to blackmailing, threatening physical harm, or invading personal privacy.

2. Cyber Bullying

Cyber bullying involves insulting, humiliating, or harassing women through digital platforms. It may include posting offensive comments, spreading rumours, sharing embarrassing content, or publicly shaming women on social media. Victims of cyber bullying often suffer from anxiety, depression, low self-esteem, and emotional trauma. Young girls and students are particularly vulnerable to this form of cyber crime.

3. Online Harassment

Online harassment includes sending obscene messages, abusive comments, threats, or sexually explicit content through emails, chats, or social networking sites. Women are frequently targeted through vulgar language, unwanted sexual advances, or threatening communication. Such harassment creates an unsafe online environment and negatively affects the dignity and mental peace of victims.

4. Identity Theft

Identity theft occurs when criminals steal personal information such as passwords, bank details, photographs, or social media credentials of women and misuse them for fraudulent purposes. Offenders may create fake accounts, conduct financial fraud, or misuse the victim's identity to commit illegal acts. Identity theft not only causes financial loss but also damages the reputation and privacy of women.

5. Morphing of Images

Morphing refers to editing or altering photographs of women using computer software to create fake or obscene images. These manipulated images are then circulated online to harass, defame, or blackmail victims. Morphing violates the dignity and privacy of women and often leads to mental stress and social embarrassment.

6. Revenge Pornography

Revenge pornography involves sharing intimate photographs or videos of women online without their consent, usually by former partners or acquaintances. The purpose is often to humiliate, threaten, or take revenge on the victim. Such acts severely affect the reputation, emotional well-

being, and social life of women. In many cases, victims face depression, social stigma, and loss of employment opportunities.

7. Sextortion

Sextortion is a form of blackmail in which offenders threaten to publish private or intimate content of women unless money, sexual favours, or other demands are fulfilled. Criminals often obtain such content through hacking, fake relationships, or deception. Sextortion causes severe psychological pressure and fear among victims.

8. Fake Social Media Profiles

Criminals sometimes create fake social media accounts in the name of women by using their photographs and personal details. These fake profiles are used to spread false information, send inappropriate messages, or damage the reputation of victims. Fake accounts may also be used to commit fraud or trap other individuals.

9. Email Spoofing and Phishing

Email spoofing involves sending fake emails that appear to come from trusted persons or organizations. Phishing refers to fraudulent attempts to obtain passwords, banking information, or confidential data through fake links or websites. Women may become victims of financial fraud, identity theft, or hacking due to such deceptive activities.

10. Cyber Defamation

Cyber defamation occurs when false, offensive, or harmful statements about a woman are published online to damage her reputation. Defamatory content may be spread through blogs, websites, social media posts, or messaging platforms. Such acts may affect personal relationships, employment opportunities, and social standing of victims.

11. Hacking

Hacking refers to unauthorized access to computers, mobile phones, emails, or social media accounts of women. Hackers may steal personal data, photographs, financial information, or confidential documents for misuse. Hacking often results in privacy violations, financial losses,

and emotional distress for victims.

12. Deepfake Technology Abuse

Deepfake technology uses artificial intelligence to create fake videos, images, or audio recordings that appear real. Criminals misuse this technology to create obscene or misleading content involving women. Deepfake videos can be used for blackmail, harassment, defamation, or spreading misinformation. This emerging form of cyber crime poses a serious threat to the privacy and dignity of women in the digital age.

Legal remedies available to victims of cyber crimes

Women who become victims of cyber crimes have various legal remedies under Indian laws. The legal framework mainly includes the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, constitutional protections, and procedural remedies available through police authorities and courts. These remedies aim to protect the privacy, dignity, reputation, and security of women in cyberspace.

1. Remedies Under the Information Technology Act, 2000

The Information Technology Act, 2000 is the primary legislation dealing with cyber offences in India. Several provisions provide protection to women against online crimes.

(A) Section 66C – Identity Theft

This section punishes any person who fraudulently uses another person's password, digital signature, or identity information. If a woman's online identity or personal information is stolen and misused, the offender may be punished with imprisonment up to three years and fine.

(B) Section 66D – Cheating by Personation

This provision applies where offenders create fake social media profiles, impersonate women online, or commit fraud through electronic communication. The punishment may extend to imprisonment up to three years along with fine.

(C) Section 66E – Violation of Privacy

Section 66E protects the privacy of individuals. It punishes capturing, publishing, or transmitting private images of a woman without her consent. This provision is particularly relevant in cases

involving hidden cameras, unauthorized sharing of photographs, and invasion of privacy.

(D) Section 67 – Publishing Obscene Material

This section punishes publication or transmission of obscene material in electronic form. It applies in cases where vulgar or offensive content relating to women is circulated online.

(E) Section 67A – Sexually Explicit Content

Section 67A deals with publishing or transmitting sexually explicit material through electronic media. It is commonly invoked in cases of revenge pornography, circulation of intimate videos, and online sexual exploitation.

(F) Section 67B – Child Sexual Content

This provision protects minor girls from online sexual exploitation and child pornography. It criminalizes the publication, transmission, or browsing of sexually explicit content involving children.

2. Remedies Under the Bharatiya Nyaya Sanhita (BNS), 2023

The Bharatiya Nyaya Sanhita contains several provisions that protect women from cyber- related offences.

(A) Sexual Harassment

Online sexual harassment through messages, images, or videos may attract punishment under provisions relating to sexual harassment.

(B) Stalking

Cyber stalking, including repeated online communication and monitoring of women through electronic means, is punishable under the law.

(C) Voyeurism

Capturing or sharing private images of women without consent constitutes voyeurism and is punishable under the BNS.

(D) Criminal Intimidation

Threatening women through emails, social media, or digital platforms amounts to criminal intimidation.

(E) Defamation

False statements, fake posts, or defamatory content published online to harm the reputation of women are punishable under defamation laws.

3. Filing of FIR and Police Complaint

Victims of cyber crimes can lodge complaints with:

- Local police station
- Cyber Crime Police Station
- National Cyber Crime Reporting Portal

Women may file a First Information Report (FIR) for cognizable offences. Police authorities have the power to investigate cybercrimes, seize digital devices, trace IP addresses, and collect electronic evidence.

4. Constitutional Remedies

Victims may also seek protection under constitutional rights guaranteed by the Constitution of India.

- Article 14 – Right to Equality
  Women are entitled to equal protection of laws against cyber offences.
- Article 19 – Freedom of Speech and Expression
  Cyber harassment and online abuse interfere with the freedom and dignity of women.
- Article 21 – Right to Life and Privacy
  The right to privacy and dignity forms part of Article 21. Cyber crimes violating personal privacy may amount to infringement of fundamental rights.

5. Civil Remedies Available to Victims

Victims may approach civil courts for:

- Compensation for mental harassment and reputational damage
- Injunction orders for removal of objectionable online content
- Protection orders restraining offenders from further harassment

Courts may direct social media platforms and websites to remove illegal or offensive material.

6. Removal and Blocking of Online Content

Victims may request removal of harmful content from:

- Social media platforms

- Websites
- Search engines
- Video-sharing applications

Intermediaries such as social media companies are required to comply with lawful directions issued by courts or government authorities for removal of unlawful content.

7. Compensation to Victims

Victims suffering financial loss, reputational injury, or emotional distress due to cyber crimes may claim compensation. Courts and adjudicating authorities may award damages depending upon the nature of harm caused.

8. Role of Cyber Cells and Investigation Agencies

Specialized cyber cells and law enforcement agencies assist victims by:

- Tracking offenders
- Recovering hacked accounts
- Preserving electronic evidence
- Blocking illegal content
- Conducting digital forensic investigation

Many states have dedicated women cyber safety units for handling complaints relating to online harassment and abuse.

9. Preventive and Protective Remedies

Victims are advised to:

- Preserve screenshots and electronic evidence
- Report offences immediately
- Change passwords and strengthen privacy settings
- Avoid sharing sensitive personal information online
- Use two-factor authentication for online accounts

These preventive measures help reduce the risk of further exploitation.

Important Case Laws on Cyber Crime Against Women in India

1. State of Tamil Nadu v. Suhas Katti (2004)

This is considered one of the first landmark cases relating to cyber crime against women in India. In this case, the accused created a fake email account in the name of a divorced woman and posted obscene and defamatory messages about her on internet groups. The victim received repeated phone calls and harassment due to these postings. The court convicted the accused under Sections 67 of the Information Technology Act and Sections 469 and 509 of the Indian Penal Code. The case is significant because it established that online harassment and publication of obscene material constitute punishable cyber offences.

2. State of West Bengal v. Animesh Boxi (2017)

This landmark case dealt with revenge pornography and online sexual exploitation. The accused uploaded intimate photographs and videos of his former girlfriend on pornographic websites after their relationship ended. He also blackmailed and threatened the victim. The court convicted the accused under Sections 354A, 354C, and 509 IPC along with Sections 66E, 67, and 67A of the Information Technology Act. The accused was sentenced to imprisonment and fine. This case is regarded as an important judicial precedent recognizing revenge pornography as a serious cyber crime against women.

3. Shreya Singhal v. Union of India (2015)

Although this case primarily challenged the constitutional validity of Section 66A of the Information Technology Act, it is important in the context of cyber crimes and online speech. The Supreme Court struck down Section 66A for violating freedom of speech under Article 19(1)(a) of the Constitution. However, the Court clarified that genuine cyber offences such as stalking, harassment, obscenity, and defamation committed through electronic means remain punishable under other legal provisions. The judgment balanced free speech with protection against online abuse.

4. Shafin Jahan v. Asokan K.M. (Right to Privacy and Online Freedom)

This case reinforced the importance of individual autonomy, dignity, and privacy, especially for

women. Though not directly a cyber crime case, the judgment emphasized that privacy and personal liberty are protected under Article 21 of the Constitution. The principles laid down are often relied upon in cyber crime matters involving online harassment, privacy violations, and unauthorized circulation of personal information.

5. K.S. Puttaswamy v. Union of India (2017)

The Supreme Court recognized the Right to Privacy as a fundamental right under Article 21 of the Constitution. This judgment has major relevance in cyber crime cases involving data theft, unauthorized sharing of private images, cyber stalking, and online surveillance of women. The decision strengthened legal protection for women against invasion of digital privacy.

6. State of Kerala v. Rakesh K. (2018)

In this case, the accused circulated a private video of a woman without her consent after the breakdown of their relationship. The court treated the act as a serious violation of privacy and dignity and held that sharing intimate content electronically without consent amounts to a punishable offence under cyber laws. The case highlighted the increasing misuse of digital technology for harassment and exploitation of women.

7. Kamlesh Vaswani v. Union of India (2013)

The petitioner sought stricter regulation and blocking of pornographic websites in India. Although the case mainly dealt with online pornography, the Supreme Court discussed concerns relating to circulation of obscene material, exploitation of women, and misuse of digital platforms. The matter emphasized the responsibility of authorities and intermediaries in regulating harmful online content.

Prevention of Cyber Crimes Against Women

Cybercrimes against women can be prevented through awareness, responsible use of technology, and effective legal enforcement. With the increasing use of social media and digital platforms, women must be educated about cyber security and safe internet practices. Awareness regarding cyber stalking, phishing, fake profiles, online harassment, and identity theft is essential to reduce

the risk of victimization. Women should avoid sharing sensitive personal information, private photographs, passwords, and banking details on online platforms. Strong passwords, privacy settings, and two-factor authentication should be used to secure social media and digital accounts. Victims should immediately report cyber offences to cyber crime cells or through the official National Cyber Crime Reporting Portal to ensure timely investigation and protection.

Effective prevention of cyber crimes against women also requires active participation of government authorities, educational institutions, families, and social media companies. Schools, colleges, and workplaces should organize cyber awareness and digital literacy programmes to educate women about online risks and safe internet usage. Parents and teachers should guide young girls regarding responsible use of social networking sites and digital platforms. Social media companies and internet intermediaries should adopt strict mechanisms for blocking fake accounts, removing abusive content, and responding quickly to complaints relating to online harassment and exploitation. Law enforcement agencies should strengthen cyber investigation units, improve digital forensic facilities, and provide specialized training to police officers for handling cyber crimes sensitively and efficiently. Public awareness campaigns, stricter implementation of cyber laws, and promotion of ethical digital behaviour are essential for creating a safe and secure cyberspace for women.

Preventive Measures Against Cyber Crimes Against Women

- Women should use strong passwords and enable two-factor authentication for online accounts.
- Personal and confidential information should not be shared on social media or with unknown persons.
- Privacy settings on social networking sites should be properly managed and updated regularly.
- Suspicious emails, links, and attachments should be avoided to prevent phishing and hacking.
- Women should preserve screenshots, chats, emails, and digital records as electronic evidence in case of cyber offences.

- Cyber crimes should be reported immediately to cyber crime cells or police authorities.
- Schools, colleges, and organizations should conduct cyber awareness and digital literacy programmes.
- Parents and teachers should educate young girls regarding safe internet practices.
- Social media platforms should promptly remove harmful, obscene, or defamatory content.
- Government authorities should strengthen cyber laws, cyber cells, and digital forensic infrastructure to ensure effective protection of women online.

Conclusion

Cyber crime against women has become one of the most significant challenges of the modern digital era. The rapid development of information technology, social media platforms, online communication systems, and digital services has provided numerous opportunities for growth and connectivity, but at the same time it has also increased the vulnerability of women to online exploitation and harassment. Crimes such as cyber stalking, cyber bullying, online harassment, identity theft, morphing of photographs, revenge pornography, sextortion, hacking, and misuse of deepfake technology have emerged as serious threats to the privacy, dignity, and security of women. These offences not only affect women financially and socially but also cause severe emotional and psychological trauma, including fear, anxiety, depression, humiliation, and loss of self-confidence. In many cases, victims hesitate to report cyber crimes because of social stigma, fear of defamation, lack of awareness, and lack of confidence in the legal system.

India has taken important steps to address cyber crimes against women through legal provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and other related laws. Various judicial decisions have also recognized the importance of protecting women's privacy, dignity, and personal liberty in cyberspace. However, despite the existence of legal remedies, challenges such as low cyber awareness, delayed investigations, inadequate cyber forensic infrastructure, cross-border nature of cyber offences, and misuse of advanced technologies continue to hinder effective enforcement. The increasing use of artificial intelligence and deepfake

technology has further complicated the nature of cyber crimes, making it more difficult to identify offenders and prevent misuse of digital content.

Therefore, combating cyber crime against women requires a comprehensive and coordinated approach involving government authorities, law enforcement agencies, educational institutions, social media companies, families, and society as a whole. Strong implementation of cyber laws, establishment of specialized cyber cells, improvement in digital forensic facilities, and speedy investigation and prosecution of cyber offences are essential for ensuring justice to victims. At the same time, women must be empowered through digital literacy, cyber awareness programmes, and knowledge of legal remedies so that they can safely use digital platforms without fear of exploitation. Social media intermediaries should also adopt strict policies for removing harmful content, blocking fake accounts, and protecting user privacy.

In conclusion, creating a safe and secure cyberspace for women is not only a legal necessity but also a social responsibility. The protection of women in the digital world is essential for ensuring equality, dignity, freedom, and human rights in modern society. Effective awareness, responsible use of technology, stronger legal enforcement, and collective social efforts are necessary to reduce cyber crimes and promote a safer digital environment for women in India.

Suggestions

Preventing cyber crimes against women requires strong legal measures, public awareness, technological safeguards, and active participation of society and government authorities. The government should strengthen and regularly update cyber laws to address emerging cyber offences such as deepfake technology, revenge pornography, online harassment, and identity theft. Specialized cyber crime police stations and women cyber safety cells should be established and equipped with advanced digital forensic facilities and trained personnel for speedy investigation of cyber offences. Law enforcement agencies, police officers, and judicial authorities should also receive proper training regarding cyber laws, handling of electronic evidence, and victim-sensitive investigation procedures to ensure effective implementation of laws and speedy justice for victims. Digital literacy and cyber awareness programmes should be conducted in schools, colleges,

workplaces, and rural areas to educate women about safe internet usage, online privacy, cyber security, and legal remedies available against cyber crimes. Women should be encouraged to use strong passwords, privacy settings, two-factor authentication, and antivirus software to protect their personal data and online accounts. They should also avoid sharing confidential information, private photographs, and banking details on digital platforms. Victims of cyber offences should be encouraged to report crimes immediately without fear of social stigma, and authorities should ensure confidentiality and protection of victims during investigation and legal proceedings.

Social media companies and internet intermediaries should adopt strict mechanisms for removing fake accounts, abusive content, obscene material, and revenge pornography from online platforms. Complaints relating to cyber harassment should be resolved promptly to prevent further harm to victims. Educational institutions should include cyber safety and ethical internet usage in academic curricula so that young people become aware of responsible digital behaviour from an early stage. Public awareness campaigns through television, newspapers, radio, and social media should also be conducted to spread knowledge regarding cyber safety and women's rights in cyberspace.

In addition, psychological counselling, legal aid, and rehabilitation support should be provided to victims of cyber crimes to help them recover from emotional and social trauma. Since many cyber offences are transnational in nature, international cooperation among countries is also necessary for tracing offenders and controlling cross-border cyber crimes. Overall, effective implementation of cyber laws, digital awareness, responsible use of technology, and collective efforts of society are essential to create a safe and secure cyberspace for women in India.

References / Bibliography

1.Books

- Cyber Laws
- Information Technology Law and Practice
- Cyber Crime: Issues, Threats and Management
- Law Relating to Computers, Internet and E-Commerce
- Cyber Crimes Against Women in India

2.Statutes and Legislations

- Information Technology Act, 2000
- Bharatiya Nyaya Sanhita, 2023
- Indian Evidence Act, 1872
- Constitution of India

3.Case Laws

- State of Tamil Nadu v. Suhas Katti
- State of West Bengal v. Animesh Boxi
- Shreya Singhal v. Union of India
- K.S. Puttaswamy v. Union of India
- Kamlesh Vaswani v. Union of India

4.Reports and Journals

- National Crime Records Bureau (NCRB) Reports on Cyber Crimes in India.
- Research articles on cybercrimes against women published in legal journals and academic databases.
- Government reports relating to women safety and cyber security.
- Articles from law journals, legal magazines, and cyber law research publications.

5.Websites and Online Sources

- [National Cyber Crime Reporting Portal](https://cybercrime.gov.in?utm_source=chatgpt.com)
- [Ministry of Electronics and Information Technology (Meitin)](https://www.meity.gov.in?utm_source=chatgpt.com)
- [National Crime Records Bureau (NCRB)](https://www.ncrb.gov.in?utm_source=chatgpt.com)
- [Indian Kanoon](https://indiankanoon.org?utm_source=chatgpt.com)
- [Cyber Dost Awareness Portal](https://cyberdost.gov.in?utm_source=chatgpt.com)