Cybercrime Against Women in India: Legal Challenges, Investigation and Emerging Trends

Kajal
Assistant Professor, Saraswati Vidya Mandir Law College, Shikarpur, UP

***Abstract*—The rapid growth of digital technology has transformed communication, education, business, and governance across the world. While technological advancements have created numerous opportunities, they have also led to a significant increase in cybercrimes targeting vulnerable sections of society, particularly women. Cybercrime against women includes offences such as cyberstalking, online harassment, identity theft, cyberbullying, revenge pornography, morphing of images, phishing, financial fraud, sextortion, and the non-consensual circulation of intimate images. The anonymity provided by the internet, coupled with the increasing use of social media platforms, has enabled offenders to commit crimes across geographical boundaries with relative ease.**

India has witnessed a substantial rise in cyber offences against women in recent years. Although several legislative measures, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and other related laws provide legal protection, challenges remain in terms of investigation, jurisdiction, digital evidence collection, and prosecution. The lack of public awareness, underreporting of offences, and inadequacies in cyber forensic infrastructure further aggravate the problem.

This paper critically examines the legal framework governing cybercrimes against women in India. It analyses the nature and forms of cyber offences, explores the effectiveness of existing laws, discusses significant judicial decisions, compares international legal approaches, and highlights the emerging challenges posed by evolving technologies such as Artificial Intelligence and Deepfake technology. The study concludes by recommending legal and policy reforms to strengthen cyber security and ensure better protection of women's rights in the digital era.

***Index Terms*—Cybercrime, Women, Cyberstalking, Information Technology Act, Digital Evidence, Online Harassment, Cyber Security, Criminal Law.**

I. INTRODUCTION

The twenty-first century is widely regarded as the digital age, where information technology has become an integral part of everyday life. Smartphones, high-speed internet, cloud computing, artificial intelligence, and social media platforms have revolutionized communication and economic development. India, with one of the largest populations of internet users globally, has experienced unprecedented digital growth through initiatives such as Digital India, online banking, e-governance, and digital education. However, the expansion of cyberspace has also created new opportunities for criminal activities.

Cybercrime refers to unlawful activities committed through computers, digital devices, or internet-based communication networks. Unlike conventional crimes, cyber offences are often committed anonymously, making the identification of offenders extremely difficult. The borderless nature of cyberspace allows criminals to target victims located in different states or even different countries. Consequently, law enforcement agencies face significant challenges in investigating and prosecuting cyber offences.

Women have emerged as one of the most vulnerable groups in cyberspace. Increasing participation in online education, professional networking, digital banking, social media, and e-commerce has exposed women to various forms of cyber victimization. Crimes such as cyberstalking, cyberbullying, identity theft, online blackmail, sextortion, revenge pornography, fake social media profiles, and circulation of morphed images have become alarmingly common. These offences often cause severe psychological trauma, social humiliation, financial loss, and reputational damage. In several instances, victims suffer depression, anxiety, and social isolation due to continuous online harassment.

The emergence of Artificial Intelligence, deepfake technology, and generative software has further complicated the nature of cybercrime. Deepfake videos and AI-generated images can be used to create false and sexually explicit content without the consent of victims. Such technological developments pose serious threats to privacy, dignity, and personal autonomy. Existing legal frameworks, many of which were enacted before these technologies became widespread, struggle to address these evolving challenges effectively.

India has enacted several laws to combat cybercrime, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and procedural safeguards under the Bharatiya Nagarik Suraksha Sanhita, 2023. Specialized institutions such as the Indian Cyber Crime Coordination Centre (I4C), Cyber Crime Cells, and the National Cyber Crime Reporting Portal have been established to facilitate reporting and investigation of cyber offences. Nevertheless, issues relating to digital evidence, cross-border jurisdiction, delayed investigations, inadequate cyber forensic laboratories, and low conviction rates continue to undermine effective enforcement.

Given the increasing dependence on digital technology and the growing incidence of cyber offences against women, there is an urgent need to evaluate the adequacy of existing legal mechanisms. A comprehensive legal framework that combines technological advancement,

effective law enforcement, judicial efficiency, public awareness, and international cooperation is essential for ensuring women's safety in cyberspace.

The present study seeks to examine the legal and practical dimensions of cybercrime against women in India by analysing statutory provisions, judicial precedents, investigative mechanisms, comparative international approaches, and emerging technological challenges.

II. REVIEW OF LITERATURE

Cybercrime against women has attracted significant attention from legal scholars, criminologists, policymakers, and international organizations in recent years. Existing literature indicates that the rapid expansion of digital technologies has substantially altered the nature of crime, requiring continuous evolution of legal frameworks and enforcement mechanisms.

Legal scholar Susan W. Brenner argues that cybercrime differs fundamentally from conventional crime because it transcends territorial boundaries, enabling offenders to exploit jurisdictional limitations and technological anonymity. According to Brenner, traditional criminal justice systems often struggle to investigate offences committed through digital networks due to the complexity of electronic evidence and cross-border cooperation.

The United Nations Office on Drugs and Crime (UNODC) has emphasized that women are disproportionately affected by technology-facilitated gender-based violence. Its reports identify online harassment, cyberstalking, non-consensual sharing of intimate images, and digital blackmail as emerging threats requiring stronger legal protection and international collaboration.

The National Crime Records Bureau (NCRB) has consistently reported an increase in cyber offences registered against women in India. These reports indicate that offences involving social media misuse, identity theft, online cheating, and publication of obscene material have grown substantially with increased internet penetration. Researchers argue that many incidents remain unreported due to social stigma, fear of retaliation, and lack of confidence in law enforcement agencies.

Indian legal scholars have examined the effectiveness of the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, in addressing cyber offences. While these statutes provide several penal provisions, many researchers contend that they were not originally designed to deal with sophisticated technologies such as artificial intelligence, encrypted communication, cryptocurrency-enabled crimes, and deepfake content. Consequently, legislative reforms have been widely recommended.

Recent studies also focus on the role of Artificial Intelligence in facilitating cyber offences. AI-powered software can generate realistic fake images, voice recordings, and videos capable of deceiving victims and investigators alike. Scholars emphasize that regulatory mechanisms governing AI-generated content are still in their infancy, creating significant legal uncertainty.

Comparative studies examining the approaches of the United States, the European Union, the United Kingdom, and Australia reveal increasing emphasis on cyber safety legislation, platform accountability, data protection, and victim support services. These jurisdictions have introduced

comprehensive legal measures to address technology-facilitated violence against women while balancing freedom of expression and digital innovation.

Overall, the literature demonstrates growing recognition that cybercrime against women is not merely a technological issue but also a serious human rights concern involving privacy, dignity, equality, and access to justice. However, significant gaps remain regarding effective implementation, digital literacy, forensic capacity, and international cooperation.

III. RESEARCH GAP

The increasing incidence of cybercrime against women has attracted considerable attention from researchers, policymakers, and legal scholars across the globe. Numerous studies have examined the legal framework governing cyber offences, digital security, and the impact of online crimes on society. However, despite the growing body of literature, several significant research gaps continue to exist, particularly in the Indian context.

Firstly, a large proportion of existing studies focus primarily on the technological aspects of cybercrime rather than examining the legal challenges faced during investigation and prosecution. While technological advancements have enabled sophisticated methods of committing cyber offences, limited research has analysed whether the existing criminal laws in India adequately address these evolving forms of digital crime.

Secondly, many studies discuss cybercrime in general without specifically focusing on crimes committed against women. Women are uniquely vulnerable to online offences such as cyberstalking, revenge pornography, sextortion, identity theft, cyberbullying, online sexual harassment, and deepfake pornography. These offences involve serious violations of privacy, dignity, reputation, and psychological well-being. However, there is insufficient scholarly work examining these gender-specific cyber offences within the framework of Indian criminal law.

Thirdly, although India has introduced the Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023, very limited academic research has examined their applicability to cyber offences against women. Most available literature continues to rely on the provisions of the Indian Penal Code, 1860, thereby creating a gap in understanding the implications of the newly enacted criminal laws.

Another important research gap relates to digital investigation and cyber forensics. Successful prosecution of cyber offences largely depends upon proper collection, preservation, and presentation of electronic evidence. However, only limited research has analysed the practical challenges encountered by investigating agencies regarding digital evidence, forensic laboratories, cross-border jurisdiction, encryption technologies, and cloud-based storage systems.

Furthermore, the rapid development of Artificial Intelligence, Deepfake technology, cryptocurrency, encrypted messaging applications, and anonymous online platforms has created entirely new forms of cybercrime. Existing legal scholarship has not adequately addressed these emerging technologies or their implications for criminal liability and victim protection.

Comparative legal analysis also remains limited. Although countries such as the United States, the United Kingdom, Australia, Singapore, and members of the European Union have adopted specialised cybercrime legislation and regulatory mechanisms, very few Indian studies comprehensively compare these approaches to identify reforms that may strengthen India's legal framework.

Finally, there remains inadequate empirical research concerning victim awareness, reporting behaviour, law enforcement preparedness, judicial efficiency, conviction rates, and rehabilitation of victims. Many cyber offences continue to go unreported due to fear of social stigma, lack of confidence in police authorities, and insufficient awareness regarding available legal remedies.

The present study seeks to bridge these research gaps by providing a comprehensive legal analysis of cybercrime against women in India. It examines existing statutory provisions, judicial precedents, investigative challenges, comparative international practices, and policy reforms necessary to strengthen cyber justice in the digital era.

IV. OBJECTIVES OF THE STUDY

The present study has been undertaken with the following objectives:

- To examine the concept and nature of cybercrime against women in India.
- To identify the major forms of cyber offences affecting women in the digital environment.
- To analyse the legal framework governing cybercrime under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and other relevant laws.
- To evaluate the effectiveness of investigative mechanisms adopted by law enforcement agencies.
- To examine the challenges associated with collection and admissibility of electronic evidence.
- To analyse important judicial decisions relating to cyber offences against women.
- To compare India's legal framework with international practices relating to cybercrime prevention.
- To identify emerging threats posed by Artificial Intelligence, Deepfake technology, cryptocurrency, and other technological developments.
- To suggest legal and policy reforms for strengthening cyber security and protection of women in cyberspace.

V. RESEARCH METHODOLOGY

The present study adopts a doctrinal and analytical research methodology. The research is primarily based upon secondary sources of information, including statutes, judicial decisions, books, research articles, government reports, committee reports, international conventions, policy papers, and publications of national and international organisations.

The principal legislations examined include the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya

Adhiniyam, 2023, and other relevant legal provisions governing cyber offences. Judicial pronouncements delivered by the Supreme Court of India and various High Courts have also been analysed to understand the judicial interpretation of cyber laws.

A comparative approach has been adopted to evaluate legal frameworks followed in countries such as the United States, the United Kingdom, Australia, Singapore, and the European Union. This comparison assists in identifying best practices that may strengthen India's cybercrime legislation.

The study further examines reports published by the National Crime Records Bureau (NCRB), the Indian Cyber Crime Coordination Centre (I4C), the United Nations Office on Drugs and Crime (UNODC), and other international organisations to understand recent trends in cybercrime against women.

An analytical approach has been employed to evaluate the effectiveness of existing laws, identify practical challenges in investigation and prosecution, and propose recommendations for future legal reforms.

VI. CONCEPT OF CYBERCRIME AGAINST WOMEN

The term cybercrime refers to any unlawful activity committed through computers, digital devices, communication networks, or the internet. Unlike conventional crimes that occur in physical spaces, cybercrimes are committed in virtual environments using electronic technologies. These offences may target individuals, organisations, governments, financial institutions, or digital infrastructure.

Cybercrime against women refers to offences committed through digital technologies that specifically target women because of their gender or exploit their personal information, identity, privacy, dignity, or reputation. Such crimes have become increasingly common with the rapid expansion of internet access, smartphones, social media platforms, online education, digital banking, and e-commerce.

The anonymity available in cyberspace enables offenders to conceal their identities while committing offences against victims located anywhere in the world. The cross-border nature of digital communication further complicates investigation and prosecution, as offenders may operate from jurisdictions beyond the reach of domestic law enforcement agencies.

Unlike traditional crimes, cyber offences often leave psychological rather than physical injuries. Victims frequently experience anxiety, depression, emotional distress, loss of self-confidence, social isolation, financial hardship, and reputational damage. In extreme cases, continuous online harassment has led to self-harm and suicide among victims.

Modern technologies such as Artificial Intelligence, machine learning, encrypted communication, cryptocurrency, and Deepfake software have further expanded the scope and sophistication of cyber offences. Criminals now employ automated tools capable of generating fake identities, realistic images, manipulated videos, phishing emails, malicious software, and fraudulent websites, making cybercrime increasingly difficult to detect.

Cybercrime against women therefore represents not merely a technological challenge but also a serious violation of fundamental human rights, including the right to privacy, dignity, equality, freedom of expression, and personal security.

6.1 Major Forms of Cybercrime Against Women

A. Cyberstalking

Cyberstalking refers to repeated and unwanted online surveillance, monitoring, communication, or harassment of a person through electronic means. Offenders frequently use emails, messaging applications, social media platforms, fake accounts, and GPS tracking to intimidate victims.

Victims often receive threatening messages, abusive comments, repeated friend requests, or unwanted video calls. Continuous online stalking creates fear, emotional trauma, and psychological distress.

B. Cyberbullying

Cyberbullying involves the repeated use of digital communication to insult, threaten, humiliate, or defame another person. It commonly occurs through social networking sites, online gaming platforms, messaging applications, and discussion forums.

Women, particularly students and young professionals, frequently become victims of body shaming, character assassination, offensive memes, and public humiliation.

C. Identity Theft

Identity theft occurs when criminals illegally obtain personal information such as Aadhaar details, bank account numbers, passwords, mobile numbers, photographs, or social media credentials for fraudulent purposes.

Stolen identities may be used to commit financial fraud, create fake social media profiles, obtain loans, or engage in criminal activities under the victim's name.

D. Morphing and Deepfake Images

Image morphing involves digitally altering photographs to create obscene or misleading content. Deepfake technology uses Artificial Intelligence to generate highly realistic fake videos or audio recordings.

Such manipulated content is frequently circulated through social media, messaging applications, or pornographic websites with the intention of humiliating women, damaging reputations, or extorting money.

The rapid growth of Deepfake technology represents one of the most serious emerging threats to women's digital safety because manipulated content often appears authentic and is difficult to distinguish from genuine recordings.

VII. TYPES OF CYBERCRIME AGAINST WOMEN IN INDIA

With the rapid advancement of digital technology, cybercrimes against women have become increasingly sophisticated and difficult to detect. The widespread use of smartphones, social networking platforms, online banking, digital payment systems, and cloud-based services has significantly expanded opportunities for cybercriminals. Unlike traditional crimes, cyber offences can be committed anonymously and often transcend national boundaries, making investigation and prosecution highly challenging. Women have become one of the most vulnerable groups in cyberspace due to increasing online participation in education, employment, business, and social networking.

The following are the major forms of cybercrime committed against women in India:

7.1 Cyberstalking

Cyberstalking refers to the repeated monitoring, tracking, or harassment of an individual through digital platforms without consent. Offenders use emails, instant messaging applications, social media accounts, GPS tracking, spyware, fake profiles, and anonymous communication tools to intimidate or threaten victims.

Cyberstalking generally begins with repeated messages, unwanted friend requests, or excessive monitoring of a person's online activities. Over time, the offender may threaten the victim, circulate false rumours, publish personal information, or attempt to establish physical contact. Victims often suffer anxiety, depression, fear, emotional distress, and disruption of their personal and professional lives.

Women journalists, celebrities, students, and professionals are particularly vulnerable to cyberstalking because of their public presence on digital platforms. The offence has become increasingly common due to the widespread availability of anonymous communication applications and encrypted messaging services.

7.2 Cyberbullying

Cyberbullying refers to repeated online behaviour intended to insult, humiliate, threaten, or emotionally abuse another person. Unlike ordinary disagreements on social media, cyberbullying involves continuous harassment that significantly affects the mental health and emotional well-being of victims.

Cyberbullies commonly post offensive comments, abusive messages, edited photographs, hateful memes, defamatory statements, or fake allegations against women through social media platforms. Educational institutions have witnessed increasing incidents of cyberbullying among students, often resulting in depression, social isolation, and even suicidal tendencies.

The permanent nature of digital content aggravates the impact of cyberbullying because offensive material can remain accessible for years and be shared repeatedly by countless users.

7.3 Identity Theft

Identity theft is one of the fastest-growing cyber offences affecting women. Criminals illegally obtain personal information such as Aadhaar numbers, PAN details, bank account information, passwords, mobile numbers, email credentials, photographs, or biometric data.

Using this information, offenders may create fake social media accounts, conduct financial fraud, obtain loans, impersonate victims, or commit criminal offences under another person's identity.

Identity theft often causes severe financial loss, reputational damage, and prolonged legal complications. Restoration of one's digital identity may require extensive legal proceedings and cooperation with multiple governmental agencies and financial institutions.

7.4 Online Sexual Harassment

Online sexual harassment includes any unwelcome sexual conduct occurring through digital communication platforms. Such behaviour includes sexually explicit messages, obscene photographs, unsolicited videos, offensive comments, repeated sexual advances, and threatening communications.

Women frequently encounter sexual harassment on social networking websites, professional networking platforms, gaming communities, online classrooms, and workplace communication systems.

The psychological consequences include humiliation, anxiety, emotional trauma, and reluctance to participate in digital activities. In many cases, victims withdraw from educational or professional opportunities because of persistent online abuse.

7.5 Revenge Pornography

Revenge pornography refers to the publication or circulation of intimate photographs or videos without the consent of the person depicted. Such material is frequently shared after the breakdown of personal relationships as a means of revenge, blackmail, or humiliation.

The rapid dissemination of intimate content through messaging applications and social media platforms causes irreparable damage to the dignity and reputation of victims. Once uploaded online, such material may remain permanently accessible despite attempts to remove it.

Victims often experience severe psychological distress, loss of employment opportunities, family disputes, social stigma, and emotional trauma. The increasing availability of anonymous file-sharing websites has made this offence particularly difficult to control.

7.6 Sextortion

Sextortion is a form of cyber-enabled blackmail in which offenders threaten to publish intimate photographs or videos unless victims provide money, additional explicit content, or sexual favours. Criminals often obtain compromising material through fake relationships, hacked devices, phishing attacks, hidden cameras, or manipulated online interactions.

Women and young girls are particularly vulnerable because offenders exploit emotional trust and social stigma associated with intimate content. Many victims avoid reporting the offence due to fear of public embarrassment and social discrimination.

7.7 Image Morphing and Deepfake Technology

Technological advancements in Artificial Intelligence have significantly increased the misuse of image editing software. Image morphing involves digitally altering genuine photographs to create obscene or misleading content.

Deepfake technology uses Artificial Intelligence algorithms to generate realistic videos or audio recordings in which an individual's face or voice is manipulated without consent.

Deepfake pornography has emerged as one of the most dangerous forms of cybercrime against women. Criminals can now create highly realistic explicit videos using publicly available photographs obtained from social media accounts.

Such content seriously violates privacy, dignity, and reputation while creating long-lasting psychological and professional consequences.

7.8 Phishing and Financial Fraud

Phishing refers to fraudulent attempts to obtain confidential information by impersonating legitimate institutions such as banks, government agencies, educational institutions, or online shopping platforms.

Women increasingly become victims of phishing through fake websites, fraudulent emails, SMS messages, QR code scams, and malicious mobile applications.

Cybercriminals use stolen banking credentials to transfer funds, make unauthorized purchases, or commit financial fraud. Digital payment systems have further increased opportunities for such offences.

VIII. LEGAL FRAMEWORK GOVERNING CYBERCRIME AGAINST WOMEN IN INDIA

India has developed a comprehensive legal framework to combat cybercrime through constitutional protections, criminal legislation, information technology laws, procedural statutes, and evidentiary rules. Although no single legislation exclusively governs cybercrime against women, several statutory provisions collectively provide protection.

8.1 Constitutional Protection

The Constitution of India guarantees several fundamental rights that protect women against cyber offences.

Article 14 guarantees equality before law and equal protection of laws.

Article 15 prohibits discrimination on the grounds of sex and empowers the State to make special provisions for women.

Article 19(1)(a) guarantees freedom of speech and expression. However, this freedom does not permit online harassment, defamation, obscenity, or hate speech.

Article 21 guarantees the right to life and personal liberty, which has been judicially interpreted to include the right to privacy, dignity, reputation, and informational self-determination.
These constitutional guarantees form the foundation for protecting women against technology-facilitated violence.

8.2 Information Technology Act, 2000
The Information Technology Act, 2000 is India's primary legislation regulating cyber activities and electronic governance. It contains several penal provisions applicable to cyber offences committed against women.

Section 66C – Identity Theft
This provision criminalizes the dishonest or fraudulent use of another person's electronic signature, password, or unique identification features.
The offence is punishable with imprisonment extending to three years along with a fine.

Section 66D – Cheating by Personation Using Computer Resources
Section 66D applies where offenders impersonate another person through digital communication to commit fraud or deception.
This provision is frequently invoked in cases involving fake matrimonial profiles, fraudulent social media accounts, online financial fraud, and impersonation.

Section 66E – Violation of Privacy
Section 66E protects individuals against unauthorized capture, publication, or transmission of private images without consent.
This provision is particularly relevant in cases involving hidden cameras, intimate photographs, and online circulation of private images.

Section 67
Section 67 criminalizes the publication or transmission of obscene material in electronic form.
It applies to websites, messaging platforms, emails, and other digital communication systems used for distributing obscene content.

Section 67A
Section 67A specifically prohibits the publication or transmission of sexually explicit material in electronic form.
The provision has become increasingly significant in cases involving revenge pornography, explicit videos, and online sexual exploitation.

Section 67B
Section 67B provides enhanced protection against child sexual abuse material and prohibits electronic publication or transmission involving minors.

Although primarily intended to protect children, it strengthens the broader legal framework governing digital sexual offences.

IX. BHARATIYA NYAYA SANHITA, 2023 AND CYBERCRIME AGAINST WOMEN

The enactment of the Bharatiya Nyaya Sanhita (BNS), 2023 marked a significant reform in India's criminal justice system by replacing the Indian Penal Code, 1860. Although the BNS does not contain a separate chapter exclusively dealing with cybercrime, many of its provisions effectively address offences committed through digital platforms. When read together with the Information Technology Act, 2000, the BNS provides a comprehensive legal framework for protecting women against technology-facilitated crimes.

Cyber offences often involve multiple criminal acts such as intimidation, extortion, identity theft, defamation, publication of obscene material, sexual harassment, and criminal intimidation. These offences are punishable under various provisions of the BNS depending upon the facts of each case.

For instance, women who receive threatening messages through social media or messaging applications may seek protection under provisions relating to criminal intimidation. Similarly, the circulation of false information intended to damage a woman's reputation may attract offences relating to defamation. Online cheating through fake matrimonial websites, fraudulent employment offers, or impersonation may also result in criminal liability under provisions dealing with cheating and fraud.

The BNS also strengthens legal protection against offences affecting women's dignity, modesty, privacy, and bodily autonomy. Courts increasingly recognize that offences committed in cyberspace may produce consequences that are as serious as conventional physical crimes.

X. BHARATIYA NAGARIK SURAKSHA SANHITA, 2023 AND INVESTIGATION OF CYBERCRIME

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, which replaced the Code of Criminal Procedure, introduces modern procedural mechanisms relevant to cybercrime investigations.

Investigation of cyber offences requires immediate preservation of electronic evidence because digital information can easily be altered, deleted, or encrypted. The BNSS enables investigating officers to collect electronic devices, obtain digital records, search cloud-based storage systems, and coordinate with internet service providers and social media platforms.

Cyber investigations generally involve the following stages:

10.1 Registration of Complaint

Victims may file complaints at:

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

- Women's Helpline
- Emergency Response Support System (112)

Immediate reporting increases the likelihood of preserving digital evidence and tracing offenders.

10.2 Collection of Digital Evidence

Investigating officers collect various forms of electronic evidence, including:

- Mobile phones
- Laptop computers
- Hard disks
- CCTV recordings
- Email records
- Chat histories
- IP addresses
- Server logs
- Social media records
- Bank transaction details
- Digital payment records

Proper documentation and maintenance of the chain of custody are essential to ensure admissibility before courts.

10.3 Digital Forensic Examination

Cyber forensic experts analyse electronic devices to recover deleted files, identify malicious software, trace internet activity, determine locations, and authenticate digital communications.

Digital forensics has become indispensable because offenders frequently attempt to erase electronic evidence after committing offences.

10.4 Filing of Charge Sheet

Upon completion of investigation, police submit the charge sheet before the competent court along with forensic reports, electronic evidence, witness statements, and expert opinions.

XI. BHARATIYA SAKSHYA ADHINIYAM, 2023 AND ELECTRONIC EVIDENCE

The Bharatiya Sakshya Adhiniyam (BSA), 2023, replacing the Indian Evidence Act, modernizes the law relating to electronic evidence.

Digital records now constitute an important category of admissible evidence in criminal proceedings.

Electronic evidence includes: Emails, WhatsApp messages, Social media conversations, Audio recordings, CCTV footage, Digital photographs, Videos, Cloud storage records, GPS data, Computer logs.

Courts increasingly rely upon digital evidence in cybercrime cases because physical evidence is often unavailable.

However, electronic evidence presents several practical challenges: Data manipulation, Hacking, Encryption, Anonymous communication, Cross-border servers, Cloud storage outside India
Consequently, proper forensic examination becomes essential before electronic records can be relied upon during trial.

XII. CHALLENGES IN INVESTIGATION OF CYBERCRIME AGAINST WOMEN

Despite legislative reforms, numerous practical challenges continue to affect cybercrime investigations.

12.1 Underreporting of Crimes

Many women hesitate to report cyber offences due to fear of social stigma, damage to reputation, family pressure, or lack of confidence in police authorities.
Underreporting prevents accurate assessment of the true extent of cybercrime in India.

12.2 Lack of Cyber Awareness

A significant proportion of internet users remain unaware of privacy settings, digital security practices, phishing techniques, password protection, and online fraud prevention.
Limited awareness increases vulnerability to cyber offences.

12.3 Cross-Border Jurisdiction

Cybercriminals frequently operate from foreign countries using anonymous servers and encrypted communication.
Jurisdictional conflicts delay investigations and require international cooperation through treaties and mutual legal assistance mechanisms.

12.4 Shortage of Cyber Experts

India continues to face shortages of trained cyber investigators, digital forensic specialists, prosecutors, and judges possessing specialized knowledge of cyber law.
Continuous capacity building remains essential.

12.5 Rapid Technological Change

Technological innovation evolves much faster than legislation.
Emerging technologies such as: Artificial Intelligence, Deepfake Software, Cryptocurrency, Blockchain, Dark Web, Internet of Things (IoT) have introduced entirely new methods of committing cyber offences that existing laws struggle to regulate effectively.

XIII. IMPORTANT JUDICIAL DECISIONS

Shreya Singhal v. Union of India (2015)

The Supreme Court declared Section 66A of the Information Technology Act unconstitutional because it violated the constitutional guarantee of freedom of speech and expression under Article 19(1)(a).

Although the judgment strengthened free speech, it reaffirmed that offences involving harassment, obscenity, criminal intimidation, and cyber exploitation remain punishable under other statutory provisions.

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

This landmark judgment recognized privacy as a Fundamental Right under Article 21 of the Constitution.

The decision has profound implications for cybercrime because digital privacy forms the foundation of protection against identity theft, unauthorized surveillance, data misuse, and online harassment.

State of Tamil Nadu v. Suhas Katti (2004)

This case remains one of India's earliest successful cybercrime convictions.

The accused used internet platforms to publish obscene and defamatory messages relating to a woman.

The case demonstrated that cyber offences could be successfully prosecuted using electronic evidence and forensic investigation.

XIV. COMPARATIVE INTERNATIONAL APPROACH

United States

The United States has enacted specialized legislation addressing cybercrime, identity theft, online fraud, and computer-related offences.

Federal agencies including the FBI investigate major cyber offences while several states have enacted laws dealing specifically with cyberstalking and revenge pornography.

United Kingdom

The United Kingdom enforces cybercrime laws through the Computer Misuse Act, Data Protection Act, and Online Safety legislation.

Recent reforms impose greater responsibility upon social media companies to remove harmful online content and protect women from digital abuse.

European Union

The European Union has adopted a comprehensive regulatory framework emphasizing: Data protection, Platform accountability, Artificial Intelligence governance, Digital Services regulation, Victim protection

The General Data Protection Regulation (GDPR) has become one of the world's strongest privacy laws.

Australia
Australia has introduced dedicated Online Safety legislation empowering regulatory authorities to remove abusive online content rapidly.
The eSafety Commissioner plays an important role in protecting women from cyber abuse, cyberbullying, and image-based exploitation.

XV. EMERGING TRENDS AND FUTURE CHALLENGES

The digital landscape is evolving at an unprecedented pace, creating new opportunities for innovation as well as new forms of cybercrime. Emerging technologies have significantly enhanced the capabilities of cybercriminals, making offences against women more sophisticated and difficult to investigate. Consequently, India's legal framework must continuously adapt to technological developments.

15.1 Artificial Intelligence (AI)

Artificial Intelligence has transformed communication, business, healthcare, education, and governance. However, AI has also become a powerful tool for cybercriminals. AI-powered software can generate convincing phishing emails, automate hacking attempts, impersonate individuals through voice cloning, and create realistic fake identities.
Women are increasingly becoming victims of AI-assisted cyber harassment, identity theft, and financial fraud. AI can also automate social engineering attacks, enabling criminals to manipulate victims into disclosing confidential information or transferring money.
The absence of specific legislation governing AI-generated criminal activities presents a significant legal challenge. Policymakers must therefore develop regulatory frameworks balancing technological innovation with individual rights and public safety.

15.2 Deepfake Technology

Deepfake technology represents one of the most dangerous developments in cybercrime against women. By using artificial intelligence, offenders can create realistic videos or audio recordings that falsely depict individuals engaging in activities they never performed.
Women have become primary targets of deepfake pornography, where publicly available photographs are manipulated into sexually explicit content. Such fabricated material spreads rapidly across social media and messaging platforms, causing severe psychological trauma, reputational damage, and emotional distress.
Current criminal laws provide only indirect protection against such offences. Therefore, dedicated legislation regulating deepfake technology is urgently required.

15.3 Dark Web

The Dark Web refers to encrypted online networks accessible only through specialized software. Criminal organizations frequently use the Dark Web for illegal trade involving stolen identities, hacked databases, malware, financial fraud, and explicit content.

Cybercriminals often purchase or sell personal information obtained from women, including photographs, passwords, banking credentials, and private communications. The anonymous nature of the Dark Web presents enormous challenges for law enforcement agencies worldwide.

15.4 Cryptocurrency and Financial Cybercrime

Cryptocurrencies have revolutionized digital finance but have also facilitated cybercrime. Anonymous digital transactions enable offenders to receive ransom payments, launder money, and conduct illegal financial activities without revealing their identities.

Women targeted through online investment scams, romance frauds, or sextortion are frequently instructed to transfer cryptocurrency because such transactions are difficult to trace.

15.5 Internet of Things (IoT)

Smart devices connected through the Internet of Things, including security cameras, smart speakers, wearable devices, and home automation systems, have introduced additional privacy concerns.

Hackers may gain unauthorized access to these devices to monitor victims, collect personal information, or conduct digital surveillance.

Women living alone are particularly vulnerable to such privacy violations.

XVI. CONCLUSION

The digital revolution has transformed modern society by creating unprecedented opportunities for communication, education, commerce, governance, and innovation. However, these technological advancements have simultaneously facilitated new forms of criminal activity that disproportionately affect women. Cyberstalking, cyberbullying, identity theft, revenge pornography, sextortion, financial fraud, deepfake technology, and online sexual harassment have emerged as significant threats to women's privacy, dignity, and security.

India has taken important legislative steps through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. Nevertheless, technological innovation continues to evolve faster than legal regulation. Artificial Intelligence, cryptocurrency, blockchain technology, and the Dark Web have introduced new challenges requiring continuous legislative adaptation.

An effective response to cybercrime against women cannot rely solely on criminal law. It requires a multidisciplinary approach involving technological innovation, digital literacy, judicial efficiency, cyber forensic capacity, international cooperation, platform accountability, and public

awareness. Victims must be encouraged to report offences without fear of social stigma while law enforcement agencies should receive adequate resources and specialized training.

A secure digital environment is essential for ensuring women's equal participation in education, employment, entrepreneurship, governance, and public life. Strengthening cyber laws, promoting responsible technological development, and protecting fundamental rights will contribute significantly toward achieving a safer and more inclusive digital society.

REFERENCES

[1] Constitution of India.
[2] Information Technology Act, 2000.
[3] Bharatiya Nyaya Sanhita, 2023.
[4] Bharatiya Nagarik Suraksha Sanhita, 2023.
[5] Bharatiya Sakshya Adhiniyam, 2023.
[6] National Crime Records Bureau (NCRB), Crime in India Report (latest edition).
[7] Ministry of Home Affairs, Government of India.
[8] Indian Cyber Crime Coordination Centre (I4C), Government of India.
[9] United Nations Office on Drugs and Crime (UNODC), Global Study on Cybercrime.
[10] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace.
[11] Jonathan Clough, Principles of Cybercrime.
[12] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[13] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[14] State of Tamil Nadu v. Suhas Katti (2004).
[15] Council of Europe, Convention on Cybercrime (Budapest Convention).
[16] General Data Protection Regulation (GDPR), European Union.
[17] NASSCOM, Cyber Security Reports.
[18] CERT-In Annual Reports.
[19] World Economic Forum, Global Cybersecurity Outlook.
[20] Various peer-reviewed journal articles on cyber law, digital privacy, and women's rights.