INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

CYBER CRIME AGAINST WOMEN: CHALLENGES AND PREVENTION

AUTHORED BY - TEJASWANI BHADORIYA[1]

Abstract

The proliferation of digital technology has significantly increased the vulnerability of women to various forms of cybercrime. Online harassment, identity theft, cyberstalking, exploitation, and other forms of abuse have become widespread, particularly in countries like India, where rapid digitization has both connected and exposed individuals to greater risks. This paper examines the multifaceted nature of cybercrimes against women, focusing on the specific challenges faced by victims, the existing legislative framework, and the gaps in law enforcement. It also analyzes the role of societal attitudes, inadequate cyber literacy, and systemic barriers in perpetuating these crimes.

Focusing on the Indian context, the paper highlights the surge in cybercrimes against women, exploring issues such as cultural stigmas, victim-blaming, limited reporting, and inadequate support systems. It further investigates recent judicial responses and case laws, such as *Shreya Singhal vs. Union of India (2015) and K.S. Puttaswamy vs. Union of India (2017),* which have shaped the legal landscape in protecting women's rights in cyberspace. Additionally, the paper explores emerging trends like sextortion, deepfake technology misuse, and online harassment, providing a critical overview of recent case studies such as the *Bulli Bai App Case (2022) and Bois Locker Room (2020).*

Through an examination of these legal and societal challenges, the paper proposes solutions for creating safer digital environments, including strengthened legislation, improved public awareness, and advancements in technological safeguards. By addressing the gaps in the existing legal framework and enhancing victim support systems, this research aims to contribute to the ongoing discourse on protecting women in the digital age, advocating for an inclusive and secure online future for all.

[1] Tejaswani Bhadoriya, B.A.LL.B ,LL.M (Pursuing PhD), Assistant Professor, Renaissance Law College, Indore (M.P.)

 ISSN: 2582-6433

Key words: Cybercrime, Women's Safety, Digial Privacy, Legislative Framework

Introduction

The rapid advancement of digital technologies has significantly transformed communication, social interaction, and business practices, offering numerous benefits across various sectors. However, this digital revolution has also given rise to an alarming increase in cybercrimes, particularly those targeting women. Cybercrimes against women encompass a wide range of illegal activities, including cyberstalking, online defamation, revenge pornography, sextortion, and hacking of social media accounts. These offenses not only violate women's privacy but also inflict severe physical, emotional, and psychological harm, often with long-lasting consequences.

The anonymity provided by the internet emboldens perpetrators, making it difficult for victims to identify them or seek justice. Despite technological advancements and legislative efforts, the issue of cybercrime targeting women remains a complex and persistent challenge. Contributing factors such as socio-cultural taboos, insufficient digital literacy, legal gaps, and weak enforcement mechanisms exacerbate the situation, leaving many victims without adequate recourse.

In India, the rapid growth of digital infrastructure and internet access has unlocked significant economic and social opportunities. However, it has also exposed women to new risks, with cybercrimes against them on the rise. These crimes exploit existing societal vulnerabilities, including patriarchal attitudes and limited awareness about online safety. From cyberstalking and online harassment to non-consensual pornography and identity theft, women in India face an increasingly hostile digital environment.

While India's digitization initiatives have contributed to national growth, they have also led to the rise of gendered cybercrimes, such as the non-consensual sharing of intimate images, online abuse, and sextortion. Although there are legal provisions in place to combat these crimes, weak enforcement and entrenched socio-cultural barriers often hinder effective resolution.

This paper seeks to explore the key issues surrounding cybercrime against women, particularly in the Indian context, and offers actionable recommendations for improvement. The research

 ISSN: 2582-6433

will address the following central questions:

1. What are the most common forms of cybercrimes against women in India?
2. What challenges hinder the effective resolution of these crimes?
3. What measures can strengthen the legal and technological framework to better protect women in cyberspace?

By examining these issues, the paper aims to contribute to the ongoing discourse on enhancing women's safety in the digital realm and advocating for a more secure and inclusive online environment.

Forms and Types of Cyber Crime Against Women

1. **Cyber stalking:** Cyberstalking refers to persistent and unwanted attention toward a victim online, resulting in harassment and intimidation. Women are particularly vulnerable to this crime, as perpetrators often exploit their personal information.[2] This type of crime frequently occurs through social media, emails, and instant messaging platforms. Victims often experience emotional distress, anxiety, and fear.[3]
2. **Revenge Pornography and Non-Consensual Pornography:** This crime involves sharing explicit images or videos of a woman without her consent, often as a form of retaliation or blackmail. It is commonly used to humiliate or control victims, and can be considered a tool for revenge.[4]
3. **Sextortion:** Sextortion occurs when perpetrators use threats of releasing intimate content to coerce victims into performing sexual acts or providing financial compensation. This form of cybercrime is often tied to online relationships or interactions that become abusive.[5]
4. **Online Harassment and Trolling**: Women, particularly those with public profiles such as activists or public figures, are disproportionately targeted by online harassment. This includes cyberbullying, hate speech, and trolling, all aimed at silencing or intimidating women.[6]

[2] Gupta, Ritu. "Cyber Crime Against Women: Rising Trend and Preventive Measures," International Journal of Cyber Criminology, 2022.
[3] National Crime Records Bureau (NCRB), Crime in India Report 2022.
[4] NCRB statistics on impersonation cases (2023).
[5] United Nations Women, "Gender and Cybercrime," 2021
[6] Sharma, Dipika. "Legal Framework for Combating Cyber Violence Against Women," Journal of Law and Technology, 2021.

 ISSN: 2582-6433

5. **Identity Theft and Financial Fraud**: Women's identities can be stolen for fraudulent purposes, such as creating fake profiles for scams or defamation. This can result in financial loss and significant reputational damage.[7]
6. **Online Grooming and Exploitation:** Predators may use the internet to lure and exploit women, especially minors, for criminal activities like human trafficking. This can occur through social media platforms, online games, or dating websites.[8]

Challenges in Addressing and Combating Cybercrime Against Women

1. **Lack of Awareness:** Many women are unaware of their rights or the legal remedies available against cybercrime. This lack of awareness leaves them vulnerable to exploitation.
2. **Underreporting and Victim Blaming:** Victims often hesitate to report cybercrimes due to fear of stigma, victim-blaming, or a lack of faith in the justice system. Fear of societal judgment can further discourage women from taking action.
3. **Anonymity of Perpetrators:** The anonymity provided by the internet complicates the identification and prosecution of offenders. Tools like VPNs and TOR browsers allow perpetrators to remain hidden, hindering investigations.
4. **Inadequate Legislation and Enforcement:** Many countries have cybercrime laws, but they often fail to address gender-specific issues. Additionally, despite frameworks like the Information Technology Act, 2000, enforcement remains weak due to technical and procedural challenges.
5. **Technological Challenges:** The rapid pace of technological advancements often outstrips the development of effective tools to track and counter cybercrimes.
6. **Inadequate Digital Literacy:** A lack of knowledge about online safety and security measures makes women particularly vulnerable to cyberattacks, leaving them ill-equipped to protect themselves in the digital space.
7. **Socio-Cultural Barriers:** In many conservative societies, discussing cybercrimes involving women can be taboo. This cultural stigma can prevent victims from reporting crimes and seeking help.
8. **Patriarchal Mindset and Bias:** Gender biases within society and law enforcement can discourage women from reporting cybercrimes or lead to less serious treatment of their cases.

[7] Internet and Mobile Association of India (IAMAI), "Digital Literacy and Safety Practices," 2023 Survey.
[8] UNODC, "Cyber Exploitation: Emerging Trends," 2022 Report.

 ISSN: 2582-6433

9. **Weak Law Enforcement Training:** The absence of specialized cybercrime units and a lack of digital forensics expertise in law enforcement agencies further hinders the timely investigation and prosecution of cybercrimes against women.
10. **Overloaded Judicial System:** The judicial system is often burdened with a backlog of cases, causing significant delays in legal proceedings. This can discourage victims from seeking justice or cause them to lose faith in the legal system.

Preventive Measures for Combating Cybercrime

1. Technological Interventions

- Development of AI tools for detecting and removing offensive content.
- Strengthening encryption and privacy controls on digital platforms.
- Advances in AI and machine learning for detecting and preventing cybercrimes, including real-time monitoring systems and anti-phishing software.

2. Awareness Campaigns

- Governments and NGOs should promote cyber literacy through workshops and campaigns.
- Educational institutions should incorporate digital safety modules in curriculums.
- Empowering women with knowledge about online safety practices, such as securing devices and accounts.[9]

3. Policy Enhancements

- Mandatory reporting mechanisms on social media platforms.
- Expedited legal remedies for cybercrime victims.
- Enacting and enforcing robust cybercrime laws with gender-sensitive provisions, ensuring continuous updates to address emerging threats.

4. Empowering Law Enforcement

- Establishing dedicated cybercrime cells with trained personnel.
- Regular training programs for police and judiciary on handling cybercrime cases.

[9] IAMAI, Digital Literacy and Safety Practices, 2023.

 ISSN: 2582-6433

5. Support Systems for Victims

- Setting up helplines and counseling centers for women affected by cybercrime.[10]
- Encouraging community reporting to reduce stigma and increase accountability.
- Establishing dedicated helplines and online reporting portals to allow women to report cybercrimes safely and anonymously.

6. Collaboration with Social Media Platforms

- Social media companies should enhance policies to prevent abuse and provide prompt redressal mechanisms for victims.

7. Promoting Cyber Hygiene

- Women should be encouraged to practice safe online behaviors, such as avoiding sharing personal information and using strong passwords.

Role of Stakeholders in Combating Cybercrimes Against Women

Various stakeholders play a critical role in tackling cybercrimes against women. Law enforcement agencies, including police and investigative bodies, need specialized training to handle cybercrime cases with sensitivity and efficiency. Educational institutions, such as schools and universities, should integrate digital safety into their curricula to raise awareness from an early age. Civil society organizations (CSOs), including NGOs and advocacy groups, provide vital support to victims and advocate for stronger policies. The private sector, especially tech companies, must prioritize user safety and collaborate with authorities to combat cyber threats effectively.

Legal Framework in India

India has established several laws to address cybercrimes, particularly those against women. Key legal provisions include:

1. Information Technology Act, 2000:

- Section 66E: Punishes the violation of privacy through unauthorized capture or transmission of images.
- Section 67: Penalizes publishing obscene material in electronic form.

[10] Mukherjee, Underreporting of Cyber Crime, 2021.

 ISSN: 2582-6433

- Section 67A: Specifically addresses the publication of sexually explicit content.
- Section 72: Protects against breaches of confidentiality and privacy.

2. Bharatiya Nyaya Sanhita, 2023:

- Section 78: Addresses stalking, including cyberstalking.
- Section 79: Penalizes acts intending to insult the modesty of a woman.
- Sections 356: Deal with defamation, including online abuse.

3. Protection of Women from Domestic Violence Act, 2005: This Act indirectly addresses aspects of digital abuse in domestic settings.

4. Recent Developments: The IT Rules, 2021, require social media platforms to take prompt action against offensive content, thereby improving accountability.

Role of Civil Society in Combating Cybercrimes

Civil society organizations (CSOs) play a vital role in addressing cybercrimes against women. They provide counseling services, conduct workshops on cyber hygiene, and act as intermediaries between victims and law enforcement agencies, offering crucial support to victims navigating the legal and technological challenges.[11]

Recommendations for Strengthening Cybersecurity:

To better protect women in the digital realm, several recommendations can be considered:

1. **Policy Overhaul:** Strengthening and updating existing laws to address emerging forms of cybercrime.
2. **Inclusion of Gender Perspective in Cybersecurity Policies:** Ensuring national cybersecurity frameworks consider the unique challenges faced by women.
3. **Promotion of Cyber Ethics:** Introducing cyber ethics education in schools to foster respectful online behavior from a young age.[12]

[11] Breakthrough India, Digital Safety Workshops for Women, 2022.
[12] NCERT, Inclusion of Cyber Safety in School Curricula, 2023.

 ISSN: 2582-6433

Judicial Responses and Recent Case Laws

- **Shreya Singhal vs. Union of India (2015):** The Supreme Court struck down Section 66A of the IT Act, which was criticized for curbing free speech but left a gap in addressing online harassment effectively.[13]
- **K.S. Puttaswamy vs. Union of India (2017):** The landmark judgment upheld the right to privacy, establishing a foundation for protecting women from digital violations.[14]
- **X vs. Y (2023):** In a recent case involving revenge porn, the Delhi High Court ordered the swift removal of explicit content and directed law enforcement to expedite investigations, signaling proactive judicial intervention.[15]

Recent Case Studies

- **Bulli Bai App Case (2022):** Women journalists and activists from minority communities were targeted by creating mock auction profiles with their images on a mobile application. This sparked outrage and highlighted the intersection of cybercrime and communal hatred.
- **Bois Locker Room (2020):** A private Instagram group involving teenage boys was exposed for sharing explicit content and planning sexual violence, raising concerns about the normalization of cyber harassment among youth.
- **Sextortion Scams (2023):** Several women reported falling victim to sextortion through manipulated videos, which led to mental trauma and financial losses.
- **Deepfake Technology Misuse:** The rise of deepfake technology has led to incidents of morphing women's images into explicit content, often without their knowledge.

Conclusion

Cybercrime against is a complex and multifaceted issue that requires a collaborative and multi-pronged approach. While digitization has provided numerous opportunities for empowerment, it has also exposed women to new forms of exploitation and harm. Addressing this challenge demands the combined efforts of government, organizations, and individuals to create a safer digital environment.

[13] Shreya Singhal vs. Union of India AIR 2015 SC 1523
[14] K.S. Puttaswamy vs. Union of India (2017) 10 SCC1
[15] Delhi High Court judgment on revenge porn (X vs. Y, 2023).

 ISSN: 2582-6433

In India, while the legal framework offers a foundation, there is an urgent need to strengthen enforcement, enhance public awareness, and build supportive systems for victims. This can be achieved through stringent laws, advanced technological solutions, and societal intervention aimed at reducing cybercrime and protecting women's autonomy and safety online.

Furthermore, empowering women with digital skills and promoting societal change to foster a safe online space are essential steps toward achieving gender equality in the digital era. With concerted efforts and the right interventions, reducing cybercrime against women and ensuring their safety and empowerment in the digital world can become a reality.

Bibliography:

1. Gupta, Ritu. "Cyber Crime Against Women: Rising Trend and Preventive Measures," International Journal of Cyber Criminology, 2022.
2. National Crime Records Bureau (NCRB), Crime in India Report 2022.
3. NCRB statistics on impersonation cases (2023).
4. United Nations Women, "Gender and Cybercrime," 2021
5. Sharma, Dipika. "Legal Framework for Combating Cyber Violence Against Women," Journal of Law and Technology, 2021.
6. Internet and Mobile Association of India (IAMAI), "Digital Literacy and Safety Practices," 2023 Survey.
7. UNODC, "Cyber Exploitation: Emerging Trends," 2022 Report.
8. IAMAI, Digital Literacy and Safety Practices, 2023.
9. Mukherjee, Underreporting of Cyber Crime, 2021.
10. Breakthrough India, Digital Safety Workshops for Women, 2022.
11. NCERT, Inclusion of Cyber Safety in School Curricula, 2023.
12. Shreya Singhal vs. Union of India AIR 2015 SC 1523
13. K.S. Puttaswamy vs. Union of India (2017) 10 SCC1
14. Delhi High Court judgment on revenge porn (X vs. Y, 2023).