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

CYBERCRIMES AGAINST WOMEN: LEGAL PROTECTIONS UNDER IT ACT AND BNS

AUTHORED BY - ANJALI CHAUDHARY

ABSTRACT

The surge in internet usage and smartphone proliferation in India has led to an unprecedented rise in cybercrimes, particularly those targeting women. From cyberstalking and online harassment to revenge pornography and morphing, digital platforms have become arenas of gendered violence that often go unreported or inadequately addressed. Despite legislative measures such as the Information Technology (IT) Act, 2000, and the recently introduced Bharatiya Nyaya Sanhita (BNS), 2023, systemic gaps persist in ensuring robust protection and justice for women. This paper investigates the scope and nature of cybercrimes against women, analyses the effectiveness of existing legal frameworks under the IT Act and BNS, and proposes comprehensive legal, institutional, and technological reforms to strengthen protections for women in the digital realm. The study combines doctrinal legal research with statistical evidence and case law to present a multidimensional understanding of the issue.

KEYWORDS: Cybercrime, Women, IT Act, BNS 2023, Gender-based Violence, Online Harassment, Legal Protections, India

1. INTRODUCTION

The digital revolution has brought about significant progress in communication, commerce, and connectivity. Nevertheless, this change has also given rise to a corresponding realm of criminal activity, particularly affecting vulnerable groups—especially women. In India, the increase in internet access and smartphone usage has coincided with a concerning surge in cybercrimes targeting women, which include a range of offences such as cyberstalking, online harassment, identity theft, voyeurism, and the unauthorised sharing of intimate content1. Unlike physical violence, these crimes frequently occur anonymously, crossing borders and leaving victims vulnerable with minimal options for recourse. Women, who already face

[1] National Crime Records Bureau. (2021). Crime in India: Statistics on Cyber Crimes. Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in

 ISSN: 2582-6433

systemic patriarchal barriers in the offline world, encounter heightened risks in the online environment where misogyny, harassment, and exploitation often remain unaddressed[2]. This digital victimisation not only infringes on personal privacy but also hinders women's full engagement in the digital economy, civic discussions, and public life. In response to these challenges, India has established legal frameworks such as the Information Technology (IAct of 20003, and more recently, the Bharatiya Nyaya Sanhita (BNS) of 2023, which seeks to modernise and replace outdated colonial criminal laws. While the IT Act offers a legal framework for addressing offences like data breaches and online obscenity, it has faced criticism for its lack of gender specificity and limited applicability. The BNS aims to address these shortcomings by providing clear definitions for crimes such as cyberstalking, doxing, and revenge pornography, which are aligned with the realities of modern digital threats. This paper examines the nature, scope, and effects of cybercrimes against women in India, assesses the strengths and weaknesses of the current legal protections under the IT Act and BNS, and underscores the necessity for comprehensive legal, institutional, and cultural reforms to guarantee women's digital safety and empowerment.

2. RESEARCH METHODOLOGY

[4]The study employs a doctrinal legal research approach, focusing on statutes, case law, and secondary literature. Primary data includes sections from the Information Technology Act, 2000, and Bharatiya Nyaya Sanhita, 2023. Secondary sources encompass academic journals, government reports, and NCRB data. Landmark cases like State v. Suhas Katti and Ritu Kohli serve as case studies to evaluate judicial responses.

Qualitative analysis is used to assess legal text interpretations and enforcement trends. Comparative perspectives are also drawn from international frameworks such as the UK's Online Safety Act and the EU's GDPR to evaluate the Indian system's relative effectiveness

2.1 Types of cybercrimes targeting women

Cybercrimes targeting women encompass a wide range of online offenses that exploit vulnerabilities linked to gender. These crimes often aim to harass, intimidate, defame, or

[2] Basu, S. (2017). Gender and Patriarchy in Cyberspace: An Analysis of Cyber Crimes Against Women in India. Journal of Law and Policy Studies, 9(2), 67–82.
[3] Ministry of Law and Justice. (2000). The Information Technology Act, 2000. Government of India. Retrieved from https://legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000

 ISSN: 2582-6433

exploit women by misusing digital platforms and technologies. Below are the primary types of cybercrimes that disproportionately affect women in India and globally:[5]

a) **Cyberstalking**

Cyberstalking involves persistently following a woman's digital presence, monitoring her online activities, and sending threatening or unsolicited messages via email, social media, or messaging apps. Offenders often exploit personal information shared online to instill fear or exert control over the victim. It can escalate to offline stalking or violence.

b) **Online Harassment and Threats**

This includes sending offensive, abusive, or sexually explicit messages, often anonymously. Women are frequent targets on social media platforms, particularly those in public roles such as activists, journalists, or politicians. Harassment ranges from vulgar comments to rape or death threats.

c) **Revenge Porn and Non-Consensual Sharing of Intimate Images**

This involves uploading or distributing intimate photos or videos of a woman without her consent, often by former partners. It is a tool of humiliation and coercion and has severe psychological and reputational consequences.

d) **Morphing and Deepfake Abuse**

Photos of women are digitally altered (morphed) or combined with sexually explicit content using AI technologies (deepfakes). These manipulated images are circulated online to defame or blackmail the victim, often anonymously.

e) **Doxing (Online Public Exposure)**

Doxing refers to publishing a woman's private information—such as address, phone number, workplace, or photos—on public platforms without consent. It often invites further harassment and endangers her physical safety.

f) **Cyberbullying and Trolling**

Cyberbullying includes mocking, defaming, or targeting women with derogatory comments repeatedly across platforms. Trolling aims to provoke emotional responses through sexist, abusive, or violent messages, and disproportionately targets women expressing strong opinions or engaging in activism.

g) **Impersonation and Fake Profiles**

[5] Verma, A. (2021). The Rising Tide of Cyberstalking and Harassment in India: A Gendered Perspective. Journal of Law and Technology,
8(2), 102–118.

 ISSN: 2582-6433

Creating fake accounts using a woman's photos and personal details to post obscene content, solicit sexual favours, or spread misinformation is a frequent offence. This is used to damage reputations or for phishing.

h) Phishing and Online Fraud

Women are increasingly targeted by phishing scams and fake job offers, especially those offering modelling or acting opportunities. These scams often lead to financial fraud or extortion.

i) Online Voyeurism

Unauthorised access to digital devices (like webcams or cloud accounts) to capture images or videos of women without their knowledge is a form of online voyeurism. This content is often sold or distributed on illicit websites.

3. REVIEW OF LITERATURERE

Several scholars and institutions have studied cybercrimes through the gender lens:

- Ahlawat & Sharma (2024) stress that while internet access has expanded opportunities, it has also amplified risks for women due to poor legal literacy and inadequate platform accountability.
- Samridhi Goyal (2022) focuses on the lack of prompt grievance redressal mechanisms and advocates for digital safety audits on social media platforms.
- Harish Yadav (2022) argues that trauma caused by online abuse is comparable to physical violence, especially given the societal repercussions in conservative communities.
- Pillai & Rout (2021) highlight how gender stereotypes in law enforcement discourage women from reporting cybercrimes, especially in rural India.
- Sharma (2023) analyses the IT Act's Section 67, pointing out its limited success in tackling emerging crimes like deepfakes, cyber flashing, and AI-generated content.
- Tripathi & Khan (2022) compare Indian laws to those in developed jurisdictions, suggesting that India lacks strong definitional clarity and cross-border cooperation tools.
- MeitY (2023) reports emphasise training deficits among police and judiciary and highlight the need for standardised digital evidence protocols.

This literature reveals a recurring call for gender-specific, enforceable, and technologically informed legal mechanisms to ensure digital justice for women.

 ISSN: 2582-6433

3.1 LEGAL FRAMEWORK UNDER IT ACT, 2000

While originally enacted to promote digital commerce, the IT Act includes several sections relevant to cybercrimes against women:[6]

- Section 66E: Punishes the violation of privacy by capturing or transmitting private images.
- Section 66C/D: Criminalise identity theft and impersonation.
- Section 67/67A: Prohibit the publishing of obscene and sexually explicit material.
- Section 72: Penalises unauthorised disclosure of personal information.

However, critics note that these sections are gender-neutral, often failing to capture the lived experiences of women victims.

3.2 LEGAL PROVISION UNDER IPC AND BNS, 2023[7]

Nature of Offence	IPC Section.	BNS 2023 Section	Notable Changes / Observations
Assault or criminal force to outrage modesty	Section 354	Section 73	Definitions largely retained, increased sentencing scope
Sexual Harassment	Section 354A	Section 74	Stricter penalties proposed; procedural clarity added
Voyeurism	Section 354C	Section 76	Includes digital voyeurism, stronger punishment regime
Stalking	Section 354D	Section 77	Gender-neutral language introduced; expanded to cover digital stalking
Rape	Sections 375, 376	Sections 63 to 70	Expanded definitions, clearer consent framework, broader recognition of rape forms
Dowry Death	Section 304B	Section 107	Scope broadened to include abetment and conspiracy

[6] Ahlawat, H., & Sharma, S. (2024). Cyber Crimes Against Women in India. ShodhKosh: Journal of Visual and Performing Arts, 5(6), 1539–1544. https://doi.org/10.29121/shodhkosh.v5.i6.2024.2430

[7] Indian Penal code, 1860.
Bharatiya Suraksha sahinta, 2023.

 ISSN: 2582-6433

Cruelty by Husband or Relatives	Section 498A	Section 85	Expanded to include psychological abuse; safeguards to prevent misuse
Acid Attack	Sections 326A, 326B	Section 122	Includes mandatory state compensation and post-incident medical/rehabilitation support
Human Trafficking	Section 370	Section 140	Broader victim categories, more stringent punishment, victim rehabilitation considered

NCRB Crime Statistics: Trends Against Women (2015–2023)

Year	Rape	Dowry Deaths	Domestic Violence	Acid attacks	Cyber Crimes Against Women
2015	34,651	7,634	113,403	249	4,600
2020	28,046	6,966	112,292	182	10,405
2023	31,516	6,220	118,537	173	15,175

4. CASE LAWS ON CYBER CRIMES AGAINST WOMEN

1. Ritu Kohli Case (2000) – First Recognised Cyber Crime Against a Woman

Facts: A software engineer used an internet chat platform to impersonate a woman named Ritu Kohli, shared her contact details, and made obscene comments under her identity.

Legal Provisions Invoked:

- Section 67, IT Act: Publishing or transmitting obscene material in electronic form.
- Section 509, IPC / now Section 78 BNS: Word, gesture or act intended to insult the modesty of a woman.

Significance: This was the first publicly recorded case of online sexual harassment in India. It highlighted the lack of awareness about cybercrime and the gaps in digital impersonation laws at the time.

2. State of Tamil Nadu v. Suhas Katti (2004)[8]

Facts: The accused posted defamatory and obscene messages about a divorced woman in a Yahoo chat group using a fake email ID. She began receiving abusive calls from strangers.

Legal Provisions Invoked:

[8] INDIAN KANOON, State of Tamil Nadu v Suhas Katti – Cyber law case in India, indiankanoon.org.

 ISSN: 2582-6433

- Section 67, IT Act: Obscene content.
- Sections 469 & 509, IPC / now Sections 78 & 79 BNS: Forgery for harming reputation; insult to modesty.

Significance: This case resulted in a historic conviction within seven months, considered one of India's earliest successes in prosecuting cybercrime. It emphasized the relevance of Section 67 of the IT Act.

3. Puri Cyber Pornography Case (2012)

Facts: Jayant Kumar Das created a fake email and profile of a journalist's wife, posting her images on pornographic websites with derogatory content and contact details.

Legal Provisions Invoked:

- Sections 66C & 66D, IT Act: Identity theft and cheating by impersonation.
- Sections 67 & 67A, IT Act: Transmission of sexually explicit content.
- BNS Equivalent: Section 76 (voyeurism), Section 78 (sexual harassment), Section 77 (stalking).

Significance: This case was Odisha's first conviction in a cyber pornography matter, showcasing how online defamation and impersonation can be prosecuted under multiple IT Act sections.

4. Dr. Prakash v. State of Tamil Nadu

Facts: A medical doctor was accused of creating pornographic videos and distributing them to various countries through the internet, involving multiple young girls.

Legal Provisions Invoked:

- Section 67, IT Act: Publishing obscene material.
- Section 67A, IT Act: Sexually explicit acts in electronic form.

Significance: The case revealed how organized networks can exploit women online. It underscored the need for international cooperation and highlighted jurisdictional challenges in cyberspace.

5. Shree Surya v. State of Kerala

Facts: A college student was persistently harassed and stalked online by an individual sending threatening messages on social media.

Legal Provisions Invoked:

- Section 354D, IPC / now Section 77 BNS: Stalking.

 ISSN: 2582-6433

- Section 66A, IT Act (now struck down): Offensive messages via communication services.

Significance: The court took a strong stance and emphasized that digital stalking is as harmful as physical stalking. This case also sparked debate over the constitutionality of Section 66A, which was later struck down in Shreya Singhal v. Union of India (2015).

6. Sushil Ansal v. State (NCT of Delhi)

Facts: The accused distributed unauthorized, sexually explicit videos of women via online platforms and was charged under both IT Act and IPC provisions.

Legal Provisions Invoked:

- Section 67A, IT Act: Publishing sexually explicit material.
- Section 354C, IPC / now Section 76 BNS: Voyeurism.
- Section 509, IPC / now Section 78 BNS: Insulting the modesty of a woman.

Significance: The court upheld a strong sentence, reinforcing that crimes involving digital violation of women's dignity must receive exemplary punishment.

7. Kalindi Charan Lenka v. State of Odisha

Facts: A man created multiple fake profiles of a woman on social media platforms and shared defamatory content, leading to harassment and reputational damage.

Legal Provisions Invoked:

- Sections 66C & 66D, IT Act: Identity theft and impersonation.
- Section 67, IT Act: Obscene content.
- Section 354D IPC / now Section 77 BNS: Cyberstalking.

Significance: The case showcased the psychological trauma caused by online defamation and the court's ability to connect IPC offenses with digital equivalents.

5. CHALLENGES IN IMPLEMENTATION

5.1 Lack of Gender-Specific Provisions in the IT Act

Although the IT Act criminalizes various cyber offenses such as hacking, identity theft, and transmission of obscene material (Sections 66C, 66D, 67, and 67A), it remains gender-neutral and fails to address the gendered nature of cybercrimes like cyberstalking, deepfake pornography, or online abuse targeting women specifically. This generality often leads to

 ISSN: 2582-6433

under-recognition of the severity and impact of such crimes on women.[9]

5.2 Fragmentation Between Legal Frameworks

The BNS, 2023 attempts to bridge some of the legislative gaps by explicitly acknowledging digital offences like cyberstalking (Section 77) and digital voyeurism (Section 76). However, a lack of coordination between provisions under BNS and the IT Act often results in confusion during prosecution, delayed investigations, or overlapping charges. This legal overlap leads to inefficiency in the justice delivery system.

5.3 Underreporting Due to Social Stigma and Fear

One of the biggest challenges is the chronic underreporting of cybercrimes by women. Many victims fear:

- Social stigma and victim-blaming.
- Retaliation by the perpetrator.
- Embarrassment due to the public nature of the offences (e.g., leaked images).
- Lack of confidence in police response or legal recourse.
- This invisibility of victims further fuels a cycle of impunity and normalisation of online abuse.

5.4 Inadequate Law Enforcement Training

Cybercrime investigations require a deep understanding of digital evidence, encryption, IP tracing, and internet protocols. However, many police personnel lack training in digital forensics. As a result, many complaints are either not taken seriously or are poorly investigated. For example:

- Failure to preserve digital trails.
- Improper seizure of devices.
- Weak FIR drafting lacking specific charges.

This leads to low conviction rates and victim dissatisfaction.

5.5 Jurisdictional and Technological Hurdles

Many platforms where cybercrimes occur (e.g., Facebook, Instagram, X) are hosted abroad. Obtaining information or takedown support from these platforms involves cross-border data

[9] Canadian Centre for Cyber Security. (2021). Cyber threats to Canadian individuals and organisations. https://cyber.gc.ca/en/guidance/cyber-threats-canadian-individuals-and-organizations

 ISSN: 2582-6433

sharing protocols, often delayed due to bureaucratic or legal barriers. Law enforcement frequently struggles to:

- Access data from foreign servers.
- Identify anonymous offenders using VPNs or proxies.
- Implement timely takedown of harmful content.

5.6 Slow Judicial Process and Lack of Fast-Track Courts

Despite the urgency and emotional distress cybercrimes cause, India lacks a robust fast-track judicial system for cyber offenses. Victims often face:

- Long waiting periods for hearings.
- Repeated adjournments.
- Lack of sensitivity during cross-examinations.

This delays justice and deters other victims from filing complaints.

5.7 Inadequate Victim Support Mechanisms

The absence of psychological counselling, legal aid, and rehabilitation services for cybercrime survivors further exacerbates trauma. Victims are often left to navigate legal complexities alone, leading to:

- Mental health breakdowns.
- Withdrawal from online spaces.
- Career or academic disruption.

There is a dire need for one-stop support centres that offer legal, psychological, and digital safety help.

5.8 Limited Public Awareness and Digital Literacy

A significant percentage of women—especially in rural or semi-urban areas—lack awareness about what constitutes cybercrime or how to report it. Digital illiteracy results in:[10]

- Delay in detecting abuse.
- Failure to report scams or threats.
- Improper preservation of evidence (screenshots, emails, metadata).

Without mass awareness programs, the reach and impact of legal protections remain limited.

[10] Times of India. (2019). India third in cybercrime, Delhi leads in crimes: NCRB. Retrieved from https://timesofindia.indiatimes.com/india/india-third-in-cybercrime-delhi-leads-in-crimes-ncrb/articleshow/71913252.cms

 ISSN: 2582-6433

6. METHOD

The method adopted for this research includes:

- Legal Text Analysis: Review of statutory provisions from IT Act, BNS, and IPC.
- Judicial Review: Examination of precedents and interpretations from cybercrime case law.
- Trend Analysis: Study of NCRB data to understand patterns.
- Comparative Study: Evaluation of India's legal framework against international standards.

All information was categorized, coded, and analysed thematically to develop a structured understanding of the issue.

7. SUGGESTIONS

7.1 Legislative Reforms

- Introduce a Digital Violence Against Women Act with gender-sensitive provisions.
- Mandate specific clauses in the IT Act addressing AI-generated content, deepfake pornography, and cyberflashing.

7.2 Institutional Upgrades

- Establish Cyber Crime Response Units with female officers and digital forensic experts.
- Launch a Central Cyber Registry to track and manage repeat offenders.

7.3 Victim Support

- Set up one-stop redressal centres offering legal, emotional, and psychological aid.
- Implement fast-track cyber courts for time-bound resolution of cases.

7.4 Public-Private Collaboration

- Compel tech companies to share real-time abuse data and respond within 24 hours.
- Develop AI-driven hate speech monitoring tools in regional languages.

7.5 Education & Literacy

- Introduce mandatory cyber ethics education in high schools and colleges.
- Encourage community awareness drives targeting rural and semi-urban populations.

 ISSN: 2582-6433

CONCLUSION:

Cybercrimes targeting women in India have surged significantly, fuelled by advancements in technology and prevailing societal gender biases. Although there are provisions under the Information Technology Act of 2000 and the more recent Bharatiya Nyaya Sanhita (BNS), 2023, the legal framework is still inadequate to tackle the intricate and evolving nature of online gender-based violence. The IT Act offers fundamental tools but lacks specificity regarding gender issues, whereas the BNS presents more robust language and penalties for offences such as cyber harassment, stalking, and revenge pornography.

Nevertheless, enforcement is hindered by low digital literacy, underreporting of incidents, and a lack of adequate cyber forensic resources. A comprehensive strategy is crucial—this includes amending laws to clearly acknowledge new cyber threats against women, enhancing enforcement through specialised training, and improving digital literacy among women. Additionally, partnerships with technology platforms and the establishment of expedited cybercrime units can facilitate quicker resolutions.

In conclusion, ensuring the safety of women in online environments transcends legal obligations; it necessitates a societal shift—transforming digital spaces into realms of dignity, freedom, and equality.

CITATIONS:

1. H. Ahlawat & S. Sharma, Cyber Crimes Against Women in India, 5(6) ShodhKosh: J. Vis. & Performing Arts 1539 (2024), https://doi.org/10.29121/shodhkosh.v5.i6.2024.2430.
2. Samridhi Goyal, Cyber Crimes Against Women and Prevention, 3(2) Chanakya L. Rev. 98 (2022).
3. Indian Penal Code, §§ 354, 354A, 354B, 354C, 354D, 375, 376, 304B, 498A, 326A, 326B, 370 (1860).
4. Bharatiya Suraksha Sanhita, §§ 73–140 (2023).
5. State of Tamil Nadu v. Suhas Katti, available at Indian Kanoon, https://indiankanoon.org/doc/1836974/.
6. Harish Yadav, Unveiling the Dark Side of Cyberspace: A Study of Cyber Crimes Against Women in India, 11(10) Int'l J. Food & Nutritional Sci. 3408 (2022).
7. Cyber Law Review, Vol. III, Issue II (July–Dec. 2022).