Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Young Women and Digital Privacy: A Socio-Legal Study of Technology-Driven Violations and Challenges in Proving Electronic Evidence

Saransh Kanojia[a]

[a]K C Law College, University of Mumbai, Mumbai, India

Received 07 May 2026; *Accepted* 08 June 2026; *Published* 12 June 2026

Young women have increasingly turned towards the use of digital technologies for purposes like communication, education, employment, and socialisation; however, their growing reliance on these technologies has led to newer and increasing threats to their privacy in cyberspace. Cases of crimes, including deepfakes, cyberstalking, impersonation, voyeurism, non-consensual image dissemination, and exploitation of personal information, have seen a sharp rise among young women in the age group of 18 to 35 years and beyond. The research utilises the socio-legal and forensic method that will combine the use of digital surveys, interviews, and doctrinal research of the Information Technology Act, 2000, along with updated Indian criminal laws, Bharatiya Nyaya Sanhita, 2023 (BNS); Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS); and Bharatiya Sakshya Adhiniyam, 2023 (BSA). The findings of a primary survey conducted among 100 respondents indicate that 45.9% suffered from violations of their digital privacy, but 48.7% of those surveyed did not report such violations to any relevant authority. Technical challenges in investigation include issues such as the loss of metadata, disappearing messages, encryption, and faulty evidence collection, thus making the evidence inadmissible or unreliable. Organisational obstacles include a lack of sufficient capacity within the cyber-police force and an insufficiently developed forensic capacity. This study underscores the critical need for gender-sensitive mechanisms, as well as better digital forensics, and suggests draft model guidelines for a framework for reform.

Keywords: *digital privacy, cybercrime, young women, electronic evidence, BNS.*

INTRODUCTION

The advent of the digital age has brought about drastic changes in the social, professional, and educational spaces of young women in India. While affordable smartphones, fast internet, and social networking sites have made communication easier than ever before, they have also made young women vulnerable to new forms of technology-enabled violations of privacy. As per research by the World Health Organisation, one in three women is bound to be subjected to some kind of violence in her life, and one in ten women has faced some form of cyber violence after turning fifteen years old.[1] The National Crime Records Bureau (NCRB) recorded an 11% increase in cases of cybercrime against women in 2022 as compared to 2021.[2]

India has done so via a series of legislative measures. The Information Technology Act of 2000 (amended in 2008), the IT Act, forms the core of India's cyber laws. Recently, the BNS, BNSS and BSA have sought to update India's criminal justice system, including its policies on cybercrime and electronic evidence. There is also the Digital Personal Data Protection Act, 2023 (DPDP Act). However, despite the seeming plethora of legislation, there continue to be gaps created by the evolution of the cyber ecosystem, which exceeds the pace of legislation.

The challenge is made worse by the volatile nature of digital evidence, which can be deleted, encrypted, and even made inadmissible, as well as organisational inefficiencies such as inadequate cyber police force and forensic capabilities. The alarming growth in the number of cybercrime cases by 400% from 2021 to 2024, from 4,52,429 cases to 22,68,346 cases, with 12,47,393 cases in the first six months of 2025 alone, calls for an urgency of addressing this crisis.[1]

The present paper undertakes a critical study of the socio-legal crisis of digital privacy violations against young women in India using a mixed-methodology approach involving both empirical data and doctrinal legal research. The paper focuses on analysing the nature of violations, assessing the efficacy of existing law, highlighting the failures in the evidence

[1] Mukesh Ranjan, 'Cybercrimes hit rural, semi-urban India hard with over 400 per cent rise' *The New Indian Express* (07 August 2025) <https://www.newindianexpress.com/nation/2025/Aug/07/cybercrimes-hit-rural-semi-urban-india-hard-with-over-400-per-cent-rise> accessed 06 May 2026; 'Government's initiatives to strengthen security of cyber ecosystem, including against ransomware and Cross-Border Cybercrime' (*PIB*, 17 December 2025) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2205047&reg=3&lang=2> accessed 06 May 2026

and institutional mechanisms involved, and putting forth a reformative model of guidelines based on the Vishakha model. Part II discusses scope and methodology; Part III discusses literature review; Part IV discusses legal framework; Part V discusses empirical analysis; Part VI discusses evidentiary issues; Part VII discusses socio-legal aspects; Part VIII discusses recommendations and guidelines; Part IX discusses conclusion.

SCOPE OF STUDY AND METHODOLOGY

The research will concentrate on young women above the age of 18 to 35 years in India who use digital technology and have faced privacy violations facilitated by technology, which can include the making of deepfakes, cyberstalking, impersonation, and voyeuristic recording of images without consent. The effectiveness of the BNS-BNSS-BSA model, along with the IT Act and DPDP Act, will be evaluated. Even though the international instruments such as the CEDAW, Istanbul, and Budapest conventions provide good guidelines, the research is based in Indian society.

The study used an integrated socio-legal research approach that employs both empirical and doctrinal methods. Empirical data were gathered using a questionnaire distributed among 100 respondents using purposive sampling. The questionnaire consisted of multiple-choice questions, a Likert scale, and open-ended questions. Interview data was also gathered from qualitative interviews with the Mumbai Police. Secondary data included statutory provisions, judicial decisions, reports from the National Crime Records Bureau and Ministry of Home Affairs, PIB reports, and scholarly articles.[2] Data analysis techniques used included frequency distribution and percentages.

Ethical measures involved total anonymity, voluntary participation, and the lack of identification of any personal data. Limitations involved a small sample size of 100 participants; limited geographical reach to only Indians; self-reporting error related to sensitive issues; and unequal responses among the categories of incidents.

[2] Shweta Sankhwar and Arvind Chaturvedi, 'WOMAN HARASSMENT IN DIGITAL SPACE IN INDIA' (2018) 118(20) International Journal of Pure and Applied Mathematics <http://www.acadpubl.eu/hub/2018-118-21/articles/21b/68.pdf> accessed 06 May 2026

LITERATURE REVIEW

The worldwide literature highlights that women have been disproportionately exposed to cyber violence. As per the reports of the World Health Organisation, one out of every ten women experiences cyber violence from the age of 15. UN Women reported in 2025 that digital violence is intensifying, yet nearly half of the world's women and girls lack adequate legal protection from digital abuse.[3] International IDEA has recognised online violence against women as a rising concern for democratic engagement, as women tend to censor themselves out of fear of being harassed online.[4]

From an Indian perspective, Sankhwar and Chaturvedi captured the unique nature of digital harassment among women in India, where anonymity, accessibility to the platform, and the culture regarding gender make the situation conducive to cyber violence. It is observed that the NCRB Crime in India reports always depict increasing trends in cybercrimes against women, which saw an 11 per cent increase from last year, according to 2022 data. The Centre for Justice and Peace have pointed out that the cybercrime victims are invisible in the Indian justice system.[5]

In terms of the evidentiary aspect, the problems of prosecution and prevention in relation to cybercrimes include the difficulty in ensuring the chain of custody for digital evidence and the requirement for compliance with certification.[6] According to a survey conducted by the Internet Freedom Foundation in 2023, 68% of people who experienced digital fraud and harassment did not report it due to mistrust of law enforcement agencies and social stigmatisation. The literature as a whole shows that there is a documented gap between legal

[3] 'Digital violence is intensifying, yet nearly half of the world's women and girls lack legal protection from digital abuse' (*UN Women*, 18 November 2025) <https://www.unwomen.org/en/news-stories/press-release/2025/11/digital-violence-is-intensifying-yet-nearly-half-of-the-worlds-women-and-girls-lack-legal-protection-from-digital-abuse> accessed 06 May 2026

[4] 'Violence against women in digital space: A growing threat to democracy' (*International IDEA*, 27 November 2025) <https://www.idea.int/blog/violence-against-women-digital-space-growing-threat-democracy> accessed 06 May 2026

[5] 'Cybercrime and the Crisis of Digital Justice: India's invisible victims online' (*Centre for Justice and Peace*, 05 November 2025) <https://cjp.org.in/cybercrime-and-the-crisis-of-digital-justice-indias-invisible-victims-online/> accessed 06 May 2026

[6] Jay Kumar Gupta and Urja Lunia, 'Cyber Crime and the Challenges of Prosecution and Prevention' (2024) 7(4) International Journal of Law Management and Humanities <https://ijlmh.com/wp-content/uploads/Cyber-Crime-and-the-Challenges-of-Prosecution-and-Prevention.pdf?pdf=1> accessed 06 May 2026

protections and the realities of young women's experiences online, and it is this gap that the present study will attempt to explore.

LEGAL FRAMEWORK: CONSTITUTIONAL FOUNDATIONS AND STATUTORY PROVISIONS

Constitutional Foundations: Privacy as a fundamental right was authoritatively recognised by the Supreme Court in Puttaswamy v Union of India (2017),[7] where a nine-judge bench unanimously held that the right to privacy is intrinsic to life and liberty under Article 21 of the Constitution. This right also applies in cyberspace with respect to informational privacy, dignity, and autonomy. Articles 14 and 15 emphasise the principle of non-discrimination, whereas Article 19(1)(a) should be reconciled with privacy rights in cyberspace.

Information Technology Act, 2000: The IT Act, as amended in 2008, forms the main legal foundation for cybercrimes. Section 43 makes any person liable under civil law for accessing computers, downloading, or causing damage to computer systems. Section 66 makes all computer-related offences criminal. Section 66D is about impersonating another person using computer resources, which can be applied in catfishing cases and fake profiles. Section 66E punishes anyone who captures, publishes, or transmits an image of any person's private parts without their consent. Sections 67 and 67A address the publication of obscene and sexually explicit material in electronic form, respectively, with Section 67A carrying enhanced penalties.

Bharatiya Nyaya Sanhita, 2023: Substantive Cyber Offences: Several provisions under the BNS have been made, which are highly relevant in addressing digital privacy violations committed against women. Under section 77, voyeurism has been criminalised, whereby capturing or publishing images of private acts or the private parts of a woman without her consent has been considered a criminal offence – the primary offence against NCII and revenge porn. Stalking has also been defined in section 78 as a crime which includes any form of monitoring a woman's use of the internet, email, or any other form of electronic communication – this provision deals directly with cyberstalking. Section 79 covers

[7] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

harassment of a woman. Section 351(4) increases penalties in cases where criminal intimidation is done through electronic communication.

Bharatiya Nagarik Suraksha Sanhita, 2023: Procedural Reforms: This BNSS introduces changes into the processes of investigation and prosecution, which have serious ramifications for the handling of digital evidence. Section 94 gives courts the power to summon documents and electronic records, which is the most important means of compelling suspects or platforms to produce digital devices and data. Section 105 requires that search and seizures be electronically recorded by audio and video means, which ensures police accountability and prevents tampering with digital evidence.

Bharatiya Sakshya Adhiniyam, 2023: Digital Evidence: BSA marks a paradigm shift in how electronic evidence is dealt with. As per section 61, any record produced in electronic form shall be considered as primary evidence. Thus, WhatsApp messages, e-mails, and even digital videos will now enjoy the same status as paper documents. The previous provision of Section 65B of the Indian Evidence Act, 1872, was quite stringent.[8]

Digital Personal Data Protection Act, 2023: The DPDP Act, 2023, offers a complete legal structure of data rights. According to Section 6, any processing of personal data should be done with the free, specific, informed, and unambiguous consent of the data subject. According to Section 12, the data principals have the right to ask for correction or deletion of their personal data, which is an exercise of the right to be forgotten.

Critical Gaps in the Legal Framework: Despite the above legal framework, some important lacunae exist. For instance, India does not have any statutory definitions of or provisions relating to the harms caused by AI, such as deepfakes, AI-created intimate imagery, and synthetic identity fraud. The BNS provisions regarding voyeurism and cyberstalking are not adequate in addressing the issue of the AI generating or manipulating the image to show a real-life person without capturing that person through human means. There are no requirements regarding the time within which the platform must act to remove the content. The gender-sensitive investigation process is not provided for under the statute.

[8] Indian Evidence Act 1872, s 65B

Table 1: Key Statutory Provisions Governing Digital Privacy Violations Against Women

Act / Law	Section	Offence / Provision	Relevance
BNS, 2023	S 77	Voyeurism	Core provision against NCII and revenge pornography
BNS, 2023	S 78	Cyberstalking	Criminalises the internet/email monitoring of women
BNS, 2023	S 79	Harassment of a woman	Addresses persistent harassment, including by digital means
BNS, 2023	S 351(4)	Criminal intimidation via electronic communication	Enhanced penalty for digital threats and intimidation
BNS, 2023	S 69	Deceit / Catfishing	Covers digital fraud leading to sexual exploitation
BNS, 2023	S 111	Organised cybercrime	Strict penalties for syndicated cyber fraud
BNSS, 2023	S 94	Summons for electronic records	Procedural tool to demand digital data from suspects/platforms

BNSS, 2023	S 105	AV recording of search/seizure	Prevents tampering of digital evidence at the collection stage
BSA, 2023	S 61	Electronic records as primary evidence	WhatsApp chats, emails and videos are directly admissible
DPDP Act, 2023	S 6	Consent for data processing	Foundational right to informational privacy and data control
DPDP Act, 2023	S 12	Right to erasure	Limited right to be forgotten for personal data
IT Act, 2000	S 66D	Impersonation via computer resources	Covers fake profiles and catfishing offences
IT Act, 2000	S 66E	Punishment for privacy violation	Covers NCII and privacy invasion via electronic transmission
IT Act, 2000	S 67A	Sexually explicit material (electronic)	Higher penalty for distribution of sexually explicit content

EMPIRICAL FINDINGS: PREVALENCE, PATTERNS AND REPORTING BEHAVIOUR

Prevalence and Forms of Digital Privacy Violations: The main survey conducted on 100 participants indicates disturbing levels of digital privacy violations. 45.9% of the participants experienced digital privacy violations, a statistic that is quite similar to WHO data stating

that about one in ten women have been subjected to cyber violence since the age of 15.[9] Of the respondents who were affected, 85.6% fell into the 19-28 years old age bracket, thus proving that young females are the main target group. The highest number of affected persons is that of students, followed by young professionals.

Impersonation using fake profiles was found to be the most frequently encountered type of violation at 48.7%, while harassment through messaging and calls came second at 43.6%. Other types included unauthorised sharing of personal information at 28.2% and cyberstalking at 23.1%. The other violations included unauthorised sharing of pictures and videos, spying and dissemination of content without consent, all at lower rates. The violations were mostly committed using social media networks such as Facebook, Instagram, and Snapchat (87.2%) and WhatsApp (41%). This was confirmed by an interview with the Mumbai Police, which stated that photo morphing was the most reported cybercrime against women.

Legal Awareness and Reporting Behaviour: Although the prevalence rate is quite high, the reporting rate is surprisingly low. Out of the total number of respondents who have been victims of the violation, 48.7% never reported to any authority. Another 32.4% only informed their family members and friends about the violation. Only 13.3% of those who were victims of the violation reported to formal institutions like cyber police stations or other legal authorities.

The reasons behind non-reporting are complex and interrelated. Firstly, the main reason was mistrust of authorities, which was soon followed by the notion that 'nothing will be done,' which was mentioned by 32.4% of non-reporters. Other reasons included the idea that the incident is 'not serious enough' and fear of being judged, stigmatised, or retaliated against, which accounted for 19%. Another reason was concern about confidentiality, mentioned by 14%.

The problem is further aggravated by awareness issues in legal matters. Alarmingly, 44% of the participants reported being either "very unaware" or "not aware at all" of the current cyber laws, while merely 14.3% identified themselves as "very aware." The majority was

[9] 'Cyber violence against women' (*European Institute for Gender Equality*) <https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en> accessed 06 May 2026

unaware of tools like the Cybercrime Reporting Portal, Helpline 1930, or the state-level e-FIR system. It aligns with the findings of the Internet Freedom Foundation study in 2023, where 68% of victims didn't report crimes due to distrust or embarrassment.

Institutional Response and Satisfaction: Among those who chose to use official institutions, levels of satisfaction are severely lacking. Amongst the 35 participants who rated their level of satisfaction, just 14.3% were satisfied with the official response. Most of them, 62.9%, were indifferent or uncertain, while 22.9% were dissatisfied. This perpetuates the cycle: low reporting rates, poor institutional response, decreased trust, and hence even lower reporting rates.

EVIDENTIARY CHALLENGES IN PROSECUTING DIGITAL PRIVACY OFFENCES

Scale of the Problem: The evidence problem that exists in cybercrime prosecution needs to be understood against the backdrop of an exponential rise in criminal activities. According to data provided by MHA, the number of cybercrime incidents reported rose by 400%, from 4,52,429 to 22,68,346 cases from 2021 to 2024, with 12,47,393 cases in just the first six months of 2025. Like cybersecurity cases, cybercrimes also grew from 10.29 lakh in 2022 to 22.68 lakh in 2024 (PIB, 2025). Such crimes consist of volatile digital evidence that is susceptible to manipulation or deletion.

Technical Barriers to Evidence Preservation: Digital evidence in the realm of cyber privacy is very fragile by nature. The metadata associated with the evidence, such as timestamps, geographical information, device ID, and access logs, gets destroyed during regular use of the device, during upgrades, or even intentionally. End-to-end encryption used by encrypted messaging apps makes third-party access to messages impossible. Disappearing messages also pose a problem since the evidence self-destructs within hours. Deepfakes, another product of AI technology, also make digital forensics very difficult for Indian investigators.

However, the chain-of-custody documentation process, which is vital in proving the authenticity and admissibility of computer evidence, is often not followed. Even with the less complicated approach taken by the BSA, proper evidence admission necessitates the proper extraction, preservation and transfer through an established chain of custody. Seizure without proper procedure, no generation of hash values during collection, and insufficient documentation of preservation all present weaknesses exploited by defence attorneys.

Jurisdictional Complexities: Cybercrime is inherently borderless in nature. The offenders often work in a cross-jurisdictional manner utilizing various means of anonymisation such as Virtual Private Networks (VPNs), proxy servers, and offshore facilities. The Indian police face difficulty in collecting evidence from foreign-based websites, which are regulated by their own jurisdictional laws. Despite being a non-signatory to the Budapest Convention against Cybercrime, any coordination with foreign-based websites is carried out through informal channels. In addition to that, the issue of jurisdiction within India also poses problems with respect to State cyber cells and I4C.

Reporting Gap and Evidence Loss: This high percentage of non-reporting cases will result in serious evidence issues. Data retention policies ensure that volatile digital artefacts like server logs, geolocation information, and message metadata get automatically deleted after a few days or weeks. A delay of just a week from the time of the crime on the part of the victim can lead to the permanent deletion of vital evidence.

THE SOCIO-LEGAL CRISIS: INTERSECTIONAL DIMENSIONS

Why Young Women are Disproportionately Targeted: The disproportionate targeting of young women online is a replication of offline gender-based violence because of the wide scope, anonymity, and low cost involved in digital technologies. It is worth noting that 98–99% of deepfake pornography involves the exploitation of women, which clearly shows the gendered aspect of the abuse. In addition, the order issued by the Bombay High Court in 2025 to restrain the AI-driven misuse of singer Asha Bhosle's voice and image is another example.

Stigma, Secondary Victimisation and Under-Reporting: Stigma acts as a major disincentive in the process of reporting. The victims of cyber sexual offences often dread the stigma that comes with such a report. The concept of secondary victimisation, where the complainant is subjected to maltreatment by the investigating authority, court, or media, is especially rampant among young female victims of cyber sexual abuse.

Institutional Apathy and Structural Barriers: However, there is an apparent difference between the infrastructure that exists on paper and the one that works effectively. The Indian government has set up the I4C in the Ministry of Home Affairs (MHA), launched Helpline 1930 and cybercrime.gov.in, enhanced cyber cells in 33 states and union territories, blocked

9.42 lakh fake SIM cards and 2.63 lakh IMEI numbers, and spent Rs 782 crore on cybersecurity (PIB, 2025). But surprisingly, only 13.3% of the respondents who faced cybercrime approached authorities, and out of them, only 14.3% were satisfied.

RECOMMENDATIONS AND PROPOSED MODEL GUIDELINES

Legal Reforms: The foremost need is to define the nature of AI-based harms through legislation. The BNS and IT Act should be updated to include specific penalties for the use of AI to generate deepfakes, AI-based non-consensual image manipulation, and non-consensual data manipulation based on an actual individual's identity. There must be provisions to tackle gender-based violence facilitated by technology, which should require that the platforms concerned respond within 24-48 hours of reporting in case of serious offences.

Institutional Reforms: Specialised AI and digital forensics units must be set up in every state, which must include gender-sensitive procedures and fast-response teams. Internal Complaints Committees set up under the POSH Act and the UGC must be granted statutory powers and finances to conduct digital forensics audits. Fast-track courts exclusively dealing with cyber violence against women must be set up in every state.

Evidentiary Reforms: Protocols relating to digital evidence need to be improved at all stages of the investigative process. Guidelines on how victims can preserve evidence by following protocols related to capturing screenshots, metadata, exporting chats, and recording URLs and timestamps need to be disseminated. It is imperative that mandatory notifications for data preservation are sent automatically to platforms when a cybercrime complaint is filed.

Awareness and Prevention: It is necessary that legal awareness campaigns be made mandatory for young women within educational institutions, colleges, and offices, with the aid of materials in multiple languages on their rights, reporting mechanisms, and preserving evidence. A digital safety certification module prior to account creation, whereby the user completes a brief course on digital privacy, consent, and cyber law, will take care of digital illiteracy.

Proposed Model Guidelines for Prevention of Digital Privacy Violations Against Women, 2025: Drawing inspiration from the landmark Vishakha v State of Rajasthan (1997)

framework,[10] this study proposes Model Guidelines for Prevention of Digital Privacy Violations Against Women, 2025, to be observed by educational institutions, workplaces, digital platforms and government agencies until appropriate comprehensive legislation is enacted.

The definition of 'Digital Privacy Violation' is broad enough to cover cases of unauthorised distribution of images and videos, impersonation and creation of fake digital personas, stalking and unwanted digital communication, release of deepfakes and altered media, threats and extortion related to personal information or explicit imagery, and misusing permissions granted in apps and geo-location services. The institution has a duty to prevent and discourage digital harassment and offer easily available procedures to address the issue and seek prosecution.

A centralised government-sponsored complaint portal accessible via mobile app and the website will facilitate a one-stop complaint process with both anonymous and identified complaints. The complaint should be automatically directed to the concerned cyber cell, the designated grievance officer of the platform, and the counsellor. Digital Safety Committees need to be established in all schools and offices, and the committee should be headed by a woman and have an external member who is an expert in digital rights and cyber law.

CONCLUSION

This research highlights an urgent socio-legal crisis involving gender, technology, and justice in India. The young women surveyed faced increasing digital privacy abuses – 45.9% of them reported facing abuse – but 48.7% chose not to report because of stigmatisation and distrust. Of those who reported their abuse, only 14.3% were satisfied with the response by the institutions. There is also an increase in cybercrimes that is expected to grow by 400% from 2021 to 2024.

The recent laws, such as the BNS, BNSS, BSA, and DPDP Acts, have brought about much-needed changes but fall short in crucial ways. There are no specific laws for AI-related cybercrimes like deepfakes. Digital evidence is usually rendered inadmissible or tampered

[10] *Vishakha & Ors v State of Rajasthan & Ors* (1997) 6 SCC 241

with. Stigma and lack of digital literacy still make it difficult for survivors to report their abuse.

The suggested reforms, such as criminalising deepfakes, mandatory platform timelines, specialised forensic units that incorporate gender sensitivity, reporting applications, public awareness campaigns, and Model Guidelines inspired by Vishakha, would pave the way towards a survivor-centred and future-ready digital justice framework.