VOLUME 7 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

UNDERREPORTING OF CYBERCRIMES AGAINST WOMEN IN INDIA: A DOCTRINAL ANALYSIS OF PROCEDURAL AND EVIDENTIARY BARRIERS UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA AND THE BHARATIYA SAKSHYA ADHINIYAM, 2023

- Kapil Singhal[1] & Prof. Dr. Vir Narayan[2]

ABSTRACT

Cybercrime against women in India is markedly and persistently underreported, a pattern documented across victimisation surveys, institutional complaint data, and doctrinal literature alike.[3] This paper undertakes a doctrinal study of the legal and procedural barriers that contribute to this underreporting, distinguishing it from the substantive-law gaps that dominate existing scholarship on cyber-crimes against women. Rather than asking whether particular offences are adequately criminalised, this paper asks why women who are victimised frequently do not, or cannot, translate that victimisation into a registered complaint capable of triggering legal protection. The study examines the procedural architecture governing complaint registration including First Information Report (FIR) registration under Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023, the Zero FIR mechanism, and the evidentiary certificate requirements for electronic records under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 and identifies the specific procedural junctures at which underreporting is generated or entrenched. Drawing on National Crime Records Bureau data and secondary victimisation literature, the paper argues that India's procedural law, notwithstanding significant recent reform, continues to impose

[1] Student at Department of Law, Vikrant University, Gwalior
[2] Professor at School of Legal Studies, Vikrant University, Gwalior
[3]Debarati Halder and K. Jaishankar, 'Cyber Victimization in India: A Baseline Survey Report' (Centre for Cyber Victim Counselling, 2010).

© 2026 International Journal of Advanced Legal Research

evidentiary and institutional burdens that fall disproportionately on women reporting technology-facilitated offences, and that these procedural barriers operate independently of, and in addition to, the well-documented socio-cultural drivers of underreporting such as stigma and fear of retaliation.

Keywords: underreporting, cyber-crime against women, FIR registration, Zero FIR, electronic evidence, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam, secondary victimisation.

1. INTRODUCTION

Official crime statistics in India present a paradox that has troubled criminologists for over a decade: registered cybercrime figures rise sharply year on year, even as independent victimisation research and institutional complaint data suggest that the great majority of women who experience online victimisation never convert that experience into a formal police complaint. The National Crime Records Bureau's Crime in India 2024 report recorded cybercrime crossing the one-lakh mark nationally for the first time, a rise of 17.9 per cent over the previous year, even as crimes against women recorded under conventional heads declined marginally.[4] Over 1.2 lakh cybercrime cases remained pending investigation and nearly 75,000 pending trial at the time of that report, pointing to significant capacity constraints even for the cases that are registered.[5] Meanwhile, the National Commission for Women's Annual Report 2023-24 recorded only 657 cybercrime-related complaints nationally a figure that, set against any plausible estimate of actual online victimisation of women in a country with over 900 million internet users, indicates a very substantial degree of underreporting.[6]

This underreporting has historically been explained primarily through socio-cultural factors: stigma, victim-blaming, fear of social or family reprisal, and lack of digital literacy.[7] These explanations remain valid and important. However, they are not the only forces at work. This paper argues that a parallel and comparatively neglected set of barriers operates at the level of

[4]National Crime Records Bureau, Crime in India 2024 (Ministry of Home Affairs, Government of India, 2026).
[5]NCRB, Crime in India 2024 (n 2).
[6]National Commission for Women, Annual Report 2023-24 (NCW, 2024).
[7]Halder and Jaishankar (n 1).

© 2026 International Journal of Advanced Legal Research

legal procedure itself the rules governing how, where, and in what form a complaint of cyber victimisation must be made, and what evidentiary threshold it must clear to be registered, investigated, and prosecuted. These procedural barriers are doctrinally tractable in a way that socio-cultural barriers are not, and are therefore an appropriate and productive object of doctrinal legal research.

India's procedural and evidentiary framework has itself undergone substantial reform in the period under study. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) replaced the Code of Criminal Procedure, 1973 with effect from 1 July 2024, recasting the law on FIR registration under Section 173.[8] The Bharatiya Sakshya Adhiniyam, 2023 (BSA) simultaneously replaced the Indian Evidence Act, 1872, recasting the law on the admissibility of electronic records under Section 63.[9] This paper examines whether these reforms have reduced, left unchanged, or in some respects entrenched the procedural barriers that discourage or defeat the reporting of cybercrimes against women.

2. LITERATURE REVIEW

The earliest and still most influential empirical work on this subject is Halder and Jaishankar's baseline survey of cyber victimisation in India, which found that a substantial majority of women respondents who had experienced online harassment or stalking had not approached the police, citing fear of social judgement, lack of confidence that police would act, and simple unfamiliarity with available remedies.[10] Subsequent literature has largely confirmed and extended this finding across different regions and demographics. A recent sociological study situated in Jammu and Kashmir found underreporting to be driven by a combination of stigma and societal pressure specific to conservative social settings, while noting that patriarchal norms and limited digital literacy were consistent contributors to women's vulnerability more broadly.[11]

[8]Bharatiya Nagarik Suraksha Sanhita 2023, s 173.
[9]Bharatiya Sakshya Adhiniyam 2023, s 63.
[10]Halder and Jaishankar (n 1).
[11]'A Sociological Study of Cybercrimes Against Women in India: Deciphering the Causes and Evaluating the Impact' (2025) Journal of Cybersecurity tyaf026, accessed 26 August 2026.

© 2026 International Journal of Advanced Legal Research

A second strand of literature focuses specifically on the gap between formal legal protection and effective enforcement. Vanitha and Rajesh Kumar's recent study concludes that although India possesses a reasonably comprehensive legislative framework spanning the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, its practical effectiveness is undermined by delayed investigations, inadequate cyber-forensic infrastructure, jurisdictional confusion, and underreporting driven by fear of stigma, victim-blaming, and low public confidence in the complaint process.[12] Commentary from policy research institutions has similarly observed that under-reporting and misclassification are structural features of India's cybercrime data, particularly for women from marginalised communities who may never report abuse because of stigma, fear of disbelief, or lack of trust in institutions.[13]

A third, more doctrinally oriented strand of scholarship addresses the procedural law governing complaint registration itself, principally the jurisprudence flowing from the Supreme Court's decision in *Lalita Kumari v. Government of Uttar Pradesh*, which established the mandatory nature of FIR registration for cognisable offences, and its subsequent codification and partial qualification under Section 173 of the BNSS.[14] Commentary on this transition has noted that Section 173(3) BNSS introduces, for offences punishable with three to seven years' imprisonment, a statutory preliminary-inquiry mechanism requiring the prior approval of an officer not below the rank of Deputy Superintendent of Police, and that the Supreme Court's own observations in the pending matter of Azad Singh Kataria v. Union of India suggest an emerging judicial reconsideration of the rigidity of mandatory registration.[15] This literature has not, however, been substantially connected to the specific procedural situation of women reporting cyber offences, a gap this paper seeks to address by reading the FIR-registration and electronic-evidence frameworks specifically against the fact pattern of technology-facilitated victimisation of women.

[12]M. Vanitha and K. Rajesh Kumar, 'Cyber Crime Against Women in India: The Gap Between Legal Protection and Effective Enforcement' (2026) International Journal of Law Language & Interdisciplinary Studies, accessed 26 August 2026.
[13]IMPRI Impact and Policy Research Institute, 'Conceptualising Cyber-Crime Against Women: Beyond Numbers and "Online Misbehaviour"' (IMPRI, 12 November 2025), accessed 26 August 2026.
[14]Lalita Kumari v Government of Uttar Pradesh (2014) 2 SCC 1.
[15]'From Lalita Kumari to Section 173(3) BNSS: Navigating the New Frontier of FIR Registration' (LiveLaw, 9 March 2026), accessed 26 August 2026.

© 2026 International Journal of Advanced Legal Research

3. STATEMENT OF THE PROBLEM

Existing literature on cybercrime against women in India has extensively documented the fact of underreporting and has offered socio-cultural explanations for it, but has not undertaken a sustained doctrinal analysis of the procedural and evidentiary law that independently shapes whether a woman's complaint is registered, investigated, and successfully prosecuted. FIR-registration procedure, jurisdictional rules, and the certificate-based regime for admitting electronic evidence are not merely neutral machinery; each imposes specific practical demands that interact with the particular characteristics of cyber offences against women anonymity of offenders, cross-jurisdictional conduct, and reliance on volatile digital evidence in ways that may systematically discourage or defeat reporting, independent of stigma or awareness.

4. OBJECTIVES OF THE STUDY

- To examine the doctrinal framework governing FIR registration for cybercrimes against women under Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023, including the Zero FIR and e-FIR mechanisms.
- To analyse the evidentiary certificate requirements for electronic records under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, and their practical implications for victims of cyber offences.
- To identify jurisdictional and procedural barriers arising from the cross-border and cross-jurisdictional character of cybercrime that specifically affect women complainants.
- To examine institutional and infrastructural constraints including case pendency and cyber-forensic capacity as procedural (rather than purely resource) barriers to effective redressal.
- To recommend procedural and institutional reforms that reduce legal and evidentiary barriers to reporting, distinct from awareness-based interventions.

© 2026 International Journal of Advanced Legal Research

5. RESEARCH QUESTIONS

- Does the FIR-registration framework under the BNSS, 2023, including Zero FIR and e-FIR, adequately accommodate the specific characteristics of cyber offences against women?
- Does the certificate-based electronic evidence regime under Section 63 of the BSA, 2023 impose a practical burden that discourages or defeats the reporting and prosecution of cybercrimes against women?
- Are jurisdictional rules for cybercrime investigation adequate to address offences that are, by their nature, frequently cross-jurisdictional or cross-border?

6. HYPOTHESES

H1: The procedural framework governing complaint registration and electronic evidence in India, notwithstanding recent codification under the BNSS and BSA, continues to impose evidentiary and jurisdictional burdens that operate as an independent barrier to the reporting of cybercrimes against women, separate from socio-cultural stigma.

H2: Institutional infrastructure for the investigation of cybercrime cyber-forensic capacity, trained personnel, and case-pendency levels remains a significant procedural constraint that discourages complainants from pursuing formal redressal even where an FIR is successfully registered.

7. RESEARCH METHODOLOGY

This study adopts a doctrinal (black-letter) research methodology, consistent with the discipline of criminology's legal-analytical tradition and with the approach adopted in the companion paper on deepfake regulation submitted alongside this study. It relies on primary legal sources the Bharatiya Nagarik Suraksha Sanhita, 2023; the Bharatiya Sakshya Adhiniyam, 2023; the Information Technology Act, 2000; the Bharatiya Nyaya Sanhita, 2023; and leading Supreme Court decisions on FIR registration and electronic evidence read alongside secondary sources

© 2026 International Journal of Advanced Legal Research

comprising peer-reviewed and institutional literature on underreporting and victimisation,[16][17][18] and official statistical publications of the National Crime Records Bureau and the National Commission for Women.[19][20] No primary empirical data has been collected; the analysis proceeds through statutory interpretation and case-law analysis, applied specifically to the procedural journey of a woman reporting a cyber offence, from first contact with the police through to the evidentiary stage of prosecution.

8. CONCEPTUAL FRAMEWORK: PROCEDURAL BARRIERS AND SECONDARY VICTIMISATION

This paper draws on the victimological concept of secondary victimisation additional harm caused not by the original offence but by the institutional response to it to frame its analysis of procedural law. Where existing literature situates secondary victimisation primarily in the attitudes of investigating officers and the social response to disclosure,[21] this paper extends the concept to the design of procedural rules themselves. A rule that conditions the admissibility of a screenshot or chat log on a certificate signed by both a device custodian and a technical expert,[22] for instance, imposes a burden that is facially neutral but falls unevenly on complainants without institutional support, a category that disproportionately includes individual women reporting harassment by anonymous or informally-known offenders rather than institutional or corporate complainants. Similarly, jurisdictional friction in a cross-border offence imposes a burden that is procedural in origin even though its practical effect may be experienced by the victim as institutional indifference. This framework allows the doctrinal analysis that follows to distinguish barriers that are attitudinal or infrastructural in nature from those that are built into the text of procedural and evidentiary law.

[16]Halder and Jaishankar (n 1).
[17]Vanitha and Rajesh Kumar (n 10).
[18]Journal of Cybersecurity (2025) (n 9).
[19]NCRB, Crime in India 2024 (n 2).
[20]NCW Annual Report 2023-24 (n 4).
[21]IMPRI (n 11).
[22]BSA 2023, s 63 (n 7).

© 2026 International Journal of Advanced Legal Research

9. PROCEDURAL AND EVIDENTIARY FRAMEWORK GOVERNING COMPLAINT REGISTRATION

9.1 FIR REGISTRATION AND THE LALITA KUMARI FRAMEWORK

The starting point for any analysis of underreporting is the law governing registration of the First Information Report. In *Lalita Kumari v. Government of Uttar Pradesh*, a Constitution Bench of the Supreme Court held that registration of an FIR is mandatory where the information received discloses the commission of a cognisable offence, and that police discretion to conduct a preliminary inquiry before registration is confined to a narrow set of categories such as matrimonial and family disputes, commercial offences, and cases involving abnormal delay.[23]

9.2 SECTION 173 OF THE BNSS AND THE NEW PRELIMINARY-INQUIRY REGIME

The Bharatiya Nagarik Suraksha Sanhita, 2023 recasts FIR registration under Section 173, retaining the mandatory registration principle from Lalita Kumari for most cognisable offences while introducing, under Section 173(3), a specific statutory preliminary-inquiry mechanism for offences punishable with imprisonment of three years or more but less than seven years.[24] Under this provision, an officer-in-charge may, with the prior permission of an officer not below the rank of Deputy Superintendent of Police, conduct a preliminary inquiry of up to fourteen days before registering an FIR.[25] A significant number of offences most commonly invoked in cybercrime complaints against women including several provisions addressing outraging modesty, stalking, and voyeurism under the Bharatiya Nyaya Sanhita, 2023[26] fall within this three-to-seven-year punishment bracket, meaning that a complainant's access to immediate, mandatory registration can depend on the specific offence invoked and its statutory sentencing range, introducing a layer of procedural discretion at precisely the point where Lalita Kumari sought to eliminate it. The Supreme Court's own oral observations in the pending matter of *Azad Singh Kataria v. Union of India*, noting a documented rise in the filing of frivolous complaints and the collateral social consequences of automatic FIR registration, suggest that this

[23]Lalita Kumari (n 12).
[24]BNSS 2023, s 173 (n 6).
[25]LiveLaw (2026) (n 13).
[26]Bharatiya Nyaya Sanhita 2023, ss 75, 77, 78, 79.

© 2026 International Journal of Advanced Legal Research

qualification of the mandatory-registration principle may deepen rather than narrow in the coming years.[27]

9.3 ZERO FIR AND E-FIR: ADDRESSING JURISDICTIONAL BARRIERS

A specific and long-standing procedural barrier to reporting cybercrime has been jurisdictional refusal police declining to register a complaint on the ground that the offence, or the server or device involved, falls outside their territorial jurisdiction. The Supreme Court had already held, in *State of Andhra Pradesh v. Punati Ramulu*, that police cannot refuse to register an FIR purely on jurisdictional grounds,[28] a principle given administrative form through the Zero FIR mechanism, under which any police station may register a cognisable offence irrespective of the place of commission, later transferring the case to the appropriate jurisdiction.[29] Section 173 of the BNSS now codifies this position expressly, establishing that information regarding a cognisable offence may be recorded irrespective of the location of the offence, and explicitly recognising electronic communication as a valid mode of furnishing that information, subject to the informant signing or authenticating the record within three days.[30] The National Cyber Crime Reporting Portal's integration with the Zero FIR mechanism for financial cyber fraud complaints represents a further practical step toward reducing jurisdictional friction, though this integration has, to date, been most fully developed for financial fraud rather than for the harassment, stalking, and image-based offences that predominate in complaints by women.[31]

9.4 ELECTRONIC EVIDENCE: SECTION 63 OF THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Perhaps the most consequential procedural barrier specific to cyber offences lies in the law of evidence. Cybercrime against women is overwhelmingly proved through electronic records screenshots, chat logs, call data, and social media metadata rather than physical or testimonial evidence. Section 63 of the BSA, 2023, which replaced Section 65B of the Indian Evidence Act,

[27]Azad Singh Kataria v Union of India, Supreme Court of India (proceedings pending, 2026).
[28]State of Andhra Pradesh v Punati Ramulu (1993) Supp (4) SCC 707.
[29]Md. Imran Wahab, 'E-Zero FIR: Digital Response to Cybercrime' (Legal Service India, 2026), accessed 26 August 2026.
[30]Wahab (n 27).
[31]Wahab (n 27).

© 2026 International Journal of Advanced Legal Research

1872 with effect from 1 July 2024, governs the admissibility of such records.[32] Consistent with the position settled by the Supreme Court in *Anvar P.V. v. P.K. Basheer* which held that the equivalent provision under the former Evidence Act was a complete code and that a certificate was mandatory, not merely directory, for the admission of secondary electronic evidence[33] and further clarified in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,*[34] Section 63 requires that a certificate accompany the electronic record at the point it is tendered in evidence.

A material change introduced by the BSA is that this certificate must now be signed both by the person responsible for the device on which the record was produced and by a technical expert, and must disclose the hash value of the record, with a prescribed two-part certificate format set out in the Schedule to the Act.[35] For an individual woman complainant seeking to rely on, for example, screenshots of harassing messages or a morphed image circulated on social media, this dual-certification requirement presents a substantially higher practical bar than the earlier regime: she must not only preserve the record but identify and engage a technical expert competent to certify its hash value and production process, a resource that is often available to institutional or corporate litigants but not to an individual complainant, particularly outside metropolitan centres. Commentary on the 2026 amendments to the certificate Schedule has itself noted persisting uncertainty regarding who qualifies as an "expert" for the purposes of Part B of the certificate, a gap that as of the time of writing remains to be authoritatively resolved by either rule-making or judicial clarification.[36] The doctrinal lineage from *State (NCT of Delhi) v. Navjot Sandhu*, which had briefly permitted electronic evidence to be proved without a certificate through general secondary-evidence principles, [37] through to the present dual-certification regime, thus reflects a trajectory of progressively more, not less, exacting evidentiary demands a trajectory that has tightened evidentiary reliability at the cost of accessibility for unrepresented or under-resourced complainants.

9.5 INSTITUTIONAL AND INFRASTRUCTURAL CONSTRAINTS

[32]BSA 2023, s 63 (n 7).
[33]Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.
[34]Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
[35]iPleaders, 'Electronic Evidence Under the BSA, 2023' (iPleaders Blog, 2 July 2026), accessed 26 August 2026.
[36]iPleaders (n 33).
[37]State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600.

© 2026 International Journal of Advanced Legal Research

Beyond the text of procedural and evidentiary law, institutional capacity operates as a further procedural barrier in practice. The NCRB's Crime in India 2024 report recorded over 1.2 lakh cybercrime cases pending investigation and close to 75,000 pending trial nationally, alongside a 17.9 per cent year-on-year rise in registered cybercrime.[38] Even where a complaint is registered, this level of pendency signals a substantial gap between registration and effective investigative action, a gap that is liable to further discourage complainants including women who have already overcome the initial barriers to registration from pursuing a case through to prosecution.

10. FINDINGS

- The Lalita Kumari principle of mandatory FIR registration remains the doctrinal foundation for women's access to the criminal justice process, but its application to cyber offences against women is qualified by Section 173(3) of the BNSS, 2023, which introduces a statutory preliminary-inquiry mechanism for offences punishable between three and seven years' imprisonment a bracket that captures several of the provisions most commonly invoked in such complaints.

- The Zero FIR and e-FIR mechanisms, now codified under Section 173 of the BNSS, represent a genuine procedural improvement in addressing jurisdictional refusal, historically a significant barrier to reporting cross-jurisdictional cyber offences, though their fullest practical integration with the National Cyber Crime Reporting Portal has so far centred on financial fraud rather than harassment or image-based offences.

- The certificate-based regime for admitting electronic evidence under Section 63 of the BSA, 2023 has become more, not less, demanding with the introduction of a dual-signature requirement involving a technical expert, creating a practical evidentiary barrier that falls disproportionately on individual, under-resourced women complainants relative to institutional litigants.

[38] NCRB, Crime in India 2024 (n 2).

© 2026 International Journal of Advanced Legal Research

- Persisting ambiguity regarding who qualifies as an "expert" for the purposes of the Section 63 certificate compounds this evidentiary barrier and has not, at the time of writing, been authoritatively resolved.
- Institutional case pendency over 1.2 lakh cybercrime cases pending investigation nationally constitutes an independent, infrastructure-based procedural barrier that operates even after a complaint is successfully registered.
- Emerging judicial reconsideration of the rigidity of mandatory FIR registration, visible in the pending Azad Singh Kataria proceedings, indicates a possible future loosening of the Lalita Kumari safeguard, with uncertain implications for complainants in cyber-harassment cases.

11. CONCLUSION

This study set out to examine whether India's procedural and evidentiary law, independent of the socio-cultural stigma extensively documented in existing literature, itself contributes to the underreporting of cybercrimes against women. The doctrinal analysis substantiates both hypotheses advanced at the outset. First, notwithstanding the codification of mandatory FIR registration and the welcome introduction of nationwide Zero FIR and e-FIR mechanisms under the BNSS, 2023, the statutory preliminary-inquiry carve-out under Section 173(3), combined with a demonstrably more exacting dual-certification regime for electronic evidence under Section 63 of the BSA, 2023, together impose evidentiary and procedural burdens that fall unevenly on individual women complainants. Second, institutional infrastructure cyber-forensic capacity and case-pendency levels in particular constitutes an independent constraint that can discourage complainants from pursuing a case even after successfully clearing the registration stage. Underreporting of cybercrimes against women in India is therefore not solely, or even primarily, a function of stigma and awareness; it is also a function of procedural design choices that are amenable to legal reform. Addressing underreporting accordingly requires attention not only to awareness campaigns and victim support but to the specific texts of the BNSS and BSA and to the institutional capacity charged with implementing them.

© 2026 International Journal of Advanced Legal Research

12. RECOMMENDATIONS

- Exclude offences most commonly invoked in complaints of cyber harassment, stalking, and image-based abuse against women from the Section 173(3) BNSS preliminary-inquiry bracket, or issue binding guidelines clarifying that such offences fall within Lalita Kumari's mandatory-registration principle without exception.
- Extend the National Cyber Crime Reporting Portal's automated Zero FIR conversion mechanism, presently developed primarily for financial fraud, to harassment, stalking, and image-based offences against women.
- Issue clarificatory rules or a Supreme Court authoritative ruling on the qualification requirements for an "expert" under Part B of the Section 63 BSA certificate, and establish a designated, accessible panel of certifying experts attached to cyber-crime cells for use by individual complainants who lack access to private technical expertise.
- Establish a simplified, presumptive-admissibility pathway for electronic evidence submitted directly through the National Cyber Crime Reporting Portal, given that such submissions are already logged with platform-level metadata at the point of complaint.
- Increase cyber-forensic staffing and reduce case-pendency through dedicated, ring-fenced budgetary allocation to State Cyber Crime Cells, with periodic public reporting of pendency specifically for offences against women.
- Introduce a statutory time-bound obligation for the completion of investigation once an FIR concerning a cyber offence against a woman has been registered, distinct from the general investigation timelines under the BNSS.

BIBLIOGRAPHY

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

© 2026 International Journal of Advanced Legal Research

2. Azad Singh Kataria v. Union of India, Supreme Court of India (proceedings pending, 2026).
3. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
4. Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
5. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
6. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
7. Halder, D., & Jaishankar, K. (2010). Cyber victimization in India: A baseline survey report. Centre for Cyber Victim Counselling.
8. IMPRI Impact and Policy Research Institute. (2025, November 12). Conceptualising cyber-crime against women: Beyond numbers and "online misbehaviour." https://www.impriindia.com/insights/cyber-crime-against-women/
9. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
10. iPleaders. (2026, July 2). Electronic evidence under the BSA, 2023. https://blog.ipleaders.in/electronic-evidence-under-the-bsa-2023/
11. Journal of Cybersecurity. (2025). A sociological study of cybercrimes against women in India: Deciphering the causes and evaluating the impact. Journal of Cybersecurity, tyaf026. https://academic.oup.com/cybersecurity/article-pdf/11/1/tyaf026/64519404/tyaf026.pdf
12. Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1 (India).
13. LiveLaw. (2026, March 9). From Lalita Kumari to Section 173(3) BNSS: Navigating the new frontier of FIR registration. https://www.livelaw.in/lawschool/articles/lalita-kumari-section1733-bnss-fir-registration-525575
14. National Commission for Women. (2024). Annual report 2023-24. NCW.
15. National Crime Records Bureau. (2026). Crime in India 2024. Ministry of Home Affairs, Government of India.
16. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
17. State of Andhra Pradesh v. Punati Ramulu, 1993 Supp (4) SCC 707 (India).
18. Social and Political Research Foundation. (2026). Crimes against women in India: Trends, challenges, and policy responses. https://sprf.in/crimes-against-women-in-india-trends-challenges-and-policy-responses/

© 2026 International Journal of Advanced Legal Research

19. Vanitha, M., & Rajesh Kumar, K. (2026). Cyber crime against women in India: The gap between legal protection and effective enforcement. International Journal of Law Language & Interdisciplinary Studies. https://www.ijllr.com/post/cyber-crime-against-women-in-india-the-gap-between-legal-protection-and-effective-enforcement
20. Wahab, M. I. (2026). E-Zero FIR: Digital response to cybercrime. Legal Service India. https://www.legalserviceindia.com/Legal-Articles/e-zero-fir-zero-fir-cybercrime-india-bnss/

© 2026 International Journal of Advanced Legal Research