

**Swami Vivekananda Advanced Journal for Research and Studies**Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X

Pg. 62–68



The Role of Artificial Intelligence in Addressing Domestic Violence: Opportunities, Risks and Legal Challenges in India

Sajal Verma

Research Scholar, Faculty of Law, University of Allahabad, Prayagraj.

Dr. Abhishek Kumar

Associate Professor, Faculty of Law, University of Allahabad, Prayagraj.

Accepted: 19/09/2026**Published: 29/09/2026****DOI: <https://doi.org/10.5281/zenodo.23038599>**

Abstract

Artificial intelligence presents a distinctive dilemma for domestic-violence law: technologies capable of improving access to protection may also intensify surveillance, coercion and evidentiary uncertainty. This article examines the conditions under which AI-assisted domestic-violence interventions can be accommodated within India's constitutional and statutory framework. Employing doctrinal analysis and a critical reading of interdisciplinary research, it distinguishes informational assistance, professional decision support and automated determinations affecting rights. The analysis considers the Protection of Women from Domestic Violence Act, 2005, the new criminal laws, electronic-evidence jurisprudence, intermediary obligations and the phased commencement of the Digital Personal Data Protection Act, 2023. It argues that technical capacity does not establish either lawful deployment or demonstrated protective effectiveness. The central contribution is a survivor-centred framework connecting necessity, contextual validation, evidentiary integrity and institutional responsibility to the consequences of each proposed application. AI may legitimately assist legal navigation, documentation and coordinated support; its outputs should not independently determine credibility, criminal liability or entitlement to protection. Meaningful human judgment, accessible remedies and non-digital alternatives remain indispensable to a rights-respecting response.

Keywords: *Artificial intelligence; domestic violence; survivor autonomy; data protection; electronic evidence; algorithmic accountability; India.*

1. Introduction and Research Method

Domestic violence exposes the inadequacy of treating the household as a sphere insulated from legal scrutiny. Its statutory recognition extends beyond bodily injury to sexual, emotional and economic abuse, directing attention to relationships of dependence and control rather than isolated incidents alone.¹ Digitisation complicates this understanding: a communication device may connect a woman with assistance while simultaneously exposing her movements, finances and conversations to an abusive partner. The relevant legal inquiry is therefore not whether technology is intrinsically emancipatory, but under what conditions it redistributes power towards the person seeking protection.

AI introduces further complexity because it can classify narratives, identify correlations and generate apparently authoritative advice. Yet these capacities must not be conflated with an ability to understand coercion or establish legal truth. Hui, Constantino and Lee's integrative review identified twenty-two studies applying machine learning to domestic violence, while emphasising limitations concerning practical application and cross-country generalisation.² The literature supports investigation of particular uses, not an assumption that an imported predictive model will improve outcomes in India. Nor does the existence of a helpline, mobile application or electronic complaint portal establish that the service actually employs AI.

The research question is whether, and on what legal conditions, AI can assist domestic-violence prevention and response without compromising autonomy, equality and procedural fairness. The article adopts a doctrinal and analytical method, examining legislation, commencement notifications, judicial decisions and selected interdisciplinary scholarship available as of 29 September 2026. It does not report interviews, experimental results or an exhaustive systematic review. Its contribution is to distinguish the assistance technology may provide from the authority institutions must retain. Existing legal obligations are separated from proposed safeguards, and technological possibilities from demonstrated effectiveness. This distinction is essential where an erroneous recommendation can affect both immediate safety and the legal position of an accused person.

2. The Indian Legal Framework and the Limits of Technological Substitution

The Protection of Women from Domestic Violence Act, 2005 (PWDVA) supplies the principal protective

framework. It recognises a woman's right to reside in the shared household and provides protection, residence, monetary, custody and compensation orders, together with interim and ex parte relief.³ These remedies cannot be reduced to a criminal-conviction model. A system trained exclusively to identify prosecutable assault would consequently miss substantial parts of the Act's protective purpose. An appropriate design question is whether technology helps a person articulate the relief required, rather than whether it can pronounce that violence has conclusively occurred.

The statute also establishes institutional roles for Protection Officers and service providers, while permitting applications through persons acting on behalf of an aggrieved woman.⁴ AI could support these institutions, but cannot acquire their statutory powers through procurement or software design. In *Hiral P. Harsora v. Kusum Narottamdas Harsora*, the Supreme Court struck down the restriction of respondents to "adult male" persons.⁵ This enlarged the category against whom relief may be sought; it did not convert the definition of the aggrieved person into a gender-neutral provision. Digital interfaces must accurately communicate these jurisdictional distinctions instead of offering universal assurances of statutory eligibility.

Criminal liability requires separate analysis. Sections 85 and 86 of the Bharatiya Nyaya Sanhita, 2023 address cruelty by a husband or his relative; section 78 addresses stalking, including specified monitoring of electronic communications, and section 351 concerns criminal intimidation.⁶ Conduct involving digital control may engage these provisions only where their particular elements are satisfied. "AI-enabled abuse" is therefore an analytical description, not a self-executing criminal charge. Conversely, the absence of a provision expressly naming an AI technique does not necessarily place harmful conduct beyond existing law.

Procedural digitisation likewise requires precision. Section 173(1) of the Bharatiya Nagarik Suraksha Sanhita, 2023 permits information concerning a cognizable offence to be conveyed electronically, irrespective of the area of occurrence, but requires electronically communicated information to be signed within three days before it is taken on record.⁷ A chatbot's acknowledgment is not equivalent to completion of this statutory process. Systems should explain the distinction between requesting assistance, submitting information to police and applying for protective relief.

3. Opportunities: Access, Documentation and Professional Assistance

The clearest potential lies in reducing informational friction. A carefully bounded, multilingual assistant could explain available remedies, identify relevant institutions and help users prepare questions for a lawyer or Protection Officer. Speech interfaces and accessible text may assist persons who face literacy or disability-related barriers. These are proposed service functions, not established findings of effectiveness. Their value would depend on accurate local information, reliable translation and genuine human referral capacity. A sophisticated interface connected to an unavailable shelter or an unattended office merely transfers institutional failure into a more persuasive digital form.

Generative systems nevertheless present a distinct reliability problem. NIST's Generative AI Profile identifies confabulation as the production of confidently presented but erroneous content.⁸ In legal assistance, this could mean a fabricated remedy, an incorrect deadline or misleading reassurance about confidentiality. A defensible architecture would retrieve information from maintained statutory and institutional sources, display those sources, distinguish uncertainty and decline unsupported conclusions. Such controls reduce rather than eliminate error. Personalised legal strategy, emergency assessment and advice with serious consequences require qualified human involvement, not a disclaimer appended to unrestricted automated advice.

Documentation offers another useful field. With appropriate authority and safeguards, AI could arrange messages chronologically, identify duplicate files, transcribe recordings or flag passages for professional examination. The objective should be organisation rather than narrative manufacture. The survivor must be able to correct transcription and translation errors, retain her own account and distinguish original material from machine-generated interpretation. An application that silently rewrites uncertainty into certainty, removes apparently inconsistent statements or imposes a standardised narrative may distort both autonomy and evidence. Useful assistance preserves ambiguity where the underlying material is ambiguous.

Risk-assessment applications warrant greater restraint. The reviewed machine-learning literature explores classification and prediction but cautions against uncritical transfer across settings and

populations.⁹ An Indian deployment would require validation against the actual outcome and population for which it is used. Predicting repeat police contact is not identical to predicting serious violence; neither necessarily identifies a person's immediate protective needs. A risk indicator may justify closer professional inquiry, but a low score cannot establish safety. The distinction between identifying information requiring attention and determining what coercive action is justified must remain explicit.

Evaluation should consequently examine completed referrals, timely access to assistance, survivor-reported safety and unintended disclosures, rather than downloads or classification accuracy alone. Comparison with existing professional practice and simpler non-AI tools is necessary to establish added value. Thresholds for intervention involve normative choices: reducing missed cases may increase intrusive false alarms. Those trade-offs should be documented rather than concealed within technical terminology. A prospective pilot should have independent oversight, a mechanism for reporting harm and predetermined conditions for suspension. No experimental scoring system should become the sole route through which an applicant can obtain assistance.

4. Dual-Use Risks: Coercive Control, Bias and Exclusion

Technology-facilitated abuse must be understood through the relationship between the parties. Freed and colleagues' qualitative research demonstrates how intimate partners exploit ordinary technologies, shared accounts and legitimate access rather than relying exclusively on sophisticated intrusion.¹⁰ Its direct implication for design is that the assumed user may not control the device or account through which assistance is delivered. Notifications, browsing histories and automated follow-up messages can reveal help-seeking. Safety planning must therefore address the abusive partner's existing access, not merely external cybersecurity threats.

Generative capabilities introduce further potential for synthetic intimate imagery, voice impersonation and manufactured communications. These risks should not obscure the fact that much digital abuse requires no AI. The relevant distinction is between the underlying coercive conduct and the technology that intensifies its reach or credibility. India's February 2026 intermediary amendments introduced obligations concerning synthetically generated information. Under amended rule 3(2)(b), intermediaries must take

reasonable and practicable removal or disabling measures within two hours of receiving qualifying complaints concerning intimate content or electronic impersonation, including artificially morphed images.¹¹ This remedy addresses circulation, not the entirety of the domestic threat.

Synthetic media also creates an asymmetry of proof. Chesney and Citron describe a “liar’s dividend”: awareness of convincing fabrication can enable genuine evidence to be dismissed as false.¹² In domestic proceedings, the resulting danger is twofold: fabricated material may injure a party, while reflexive suspicion may discredit authentic accounts. Courts should avoid both automatic acceptance and categorical distrust. The evidentiary response requires reasoned authentication proportionate to the dispute, without imposing an impossible technological burden on a person seeking urgent protection.

Bias presents a less visible danger. As an analytical matter, training on recorded complaints risks modelling institutional visibility rather than the full distribution of violence. A person absent from administrative records may be unprotected, not safe. Dialect, disability, economic dependence and indirect expressions of fear could also affect classification in ways requiring local investigation. These are risks to be tested, not findings established for every model. Under Article 14, a public authority cannot treat technical uniformity as an adequate answer to arbitrary differentiation.¹³ A seemingly neutral score requires scrutiny of its inputs, error distribution and institutional consequences.

Exclusion may arise before an algorithm operates. A digital-only service assumes access to a usable device, a safe opportunity to communicate and sufficient comprehension of the interface. The appropriate response is not to classify those unable to participate as resistant or unreliable. Assisted access, accessible formats and face-to-face alternatives should remain available. Most importantly, automated outreach should not contact relatives or police merely because software infers danger: escalation needs a lawful basis, a context-sensitive safety assessment and attention to applicable reporting or emergency duties.

5. Privacy, Consent and the Transitional Data-Protection Regime

In *K.S. Puttaswamy v. Union of India*, the Supreme Court recognised privacy as a fundamental right, encompassing dignity and autonomy, and articulated legality, legitimate aim and proportionality as

conditions governing State intrusion.¹⁴ Applied to domestic-violence technology, this requires examination of the particular interference rather than reliance on a general protective objective. Offering information differs fundamentally from continuously analysing household communications. A public authority should identify its legal power, demonstrate why the proposed collection is necessary and consider less intrusive means. The benevolence of the objective does not itself supply lawful authority.

Temporal accuracy is especially important in discussing the Digital Personal Data Protection Act, 2023 (DPDP Act). The commencement notification dated 13 November 2025 brought specified institutional provisions into force but deferred most substantive processing obligations and individual rights until eighteen months after publication. The 2025 Rules also adopt phased commencement.¹⁵ Accordingly, as of this article’s research date, the central consent-and-rights framework cannot be described as fully operational. The following discussion concerns the enacted framework and preparation for its substantive commencement, not an assertion that all its duties are presently enforceable. During the transition, section 43A of the Information Technology Act, 2000 and the 2011 sensitive-personal-data rules remain relevant to covered bodies corporate, alongside constitutional and other applicable duties; their scope is not identical to that of the DPDP Act.¹⁶

That framework recognises consent and specified legitimate uses, provides security and accuracy obligations, and contains exemptions relevant to legal claims, judicial functions and offence-related processing. Notably, section 17(1) preserves the obligations in sections 8(1) and 8(5) within its specified exemptions.¹⁷ A protection programme therefore needs a purpose-specific legal analysis; neither “consent” nor “law enforcement” answers every question. The Act’s rights provisions also do not expressly establish a general right equivalent to a prohibition on solely automated consequential decisions.¹⁸ Data compliance alone consequently cannot resolve the separate questions of decisional fairness and lawful institutional power.

Consent must additionally be assessed against coercive conditions. An affirmative click cannot establish that an abusive partner was absent or that refusal was realistically possible. Systems should separate necessary service processing from optional analytics and model training, and should not condition

urgent assistance on unrelated reuse. Consent withdrawal, evidentiary preservation and legally required retention must be explained together rather than through contradictory promises. These design proposals supplement, rather than replace, the statutory inquiry into the basis and limits of processing.

Privacy protection also requires disciplined architecture: restricted access, encryption, short retention where lawful, safe contact preferences and separation of identity information from analytical datasets. Identifiable narratives should not enter general-purpose training pipelines merely because they were supplied for assistance. Children's information and shelter locations require particular operational caution. More data is not invariably more protection; unnecessary collection creates additional opportunities for disclosure and misuse. The governing question is whether each processing operation serves an identified protective function that cannot reasonably be achieved with less exposure.

6. Electronic Evidence and Procedural Fairness

AI complicates evidence at three distinct levels: organising an existing record, altering its presentation and generating new material. Sections 61–63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) govern electronic-record proof, with section 63 and its Schedule addressing computer outputs and certification.¹⁹ The admissibility of the relevant output must be established through the applicable statutory route; a software-generated report is not self-authenticating. In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court explained certification under section 65B of the former Evidence Act.²⁰ That decision remains important to the doctrinal background but must not be represented as an interpretation of the subsequently enacted BSA.

The transition between evidence statutes has practical consequences for AI-assisted legal services. Section 170(2) of the BSA preserves the former Evidence Act for the pending matters specified in its saving clause.²¹ A system that simply replaces every reference to section 65B with section 63 may therefore misstate the governing law. Document-assistance tools need procedural-history checks and professional verification. Currency is not merely a matter of retrieving the newest statute; it requires determining which enactment governs the particular proceeding.

Preservation should maintain the original file, available metadata, acquisition history and a record of

subsequent transformations. Hashing can assist verification that a captured file has not changed; it does not prove that the depicted event originally occurred.²² AI-enhanced audio or imagery should therefore be accompanied by the unaltered material and an explanation of the process used. Neither a confident transcript nor an automated authenticity score should foreclose challenge. Provenance, contextual corroboration and expert examination remain distinct questions from whether an algorithm describes a file as genuine.

The Supreme Court's decision in *Vibhor Garg v. Neha* illustrates the need for contextual analysis. The Court permitted secretly recorded spousal conversations to be taken on record in matrimonial proceedings, addressing the marital-communications exception and the Family Court's evidentiary powers.²³ It did not establish that every recording is authentic or that all methods of obtaining private information are lawful. Admissibility, weight, privacy and the legality of acquisition must not be collapsed into a single proposition. The judgment is not a general licence for protective applications to conduct covert surveillance.

Procedural fairness also concerns how algorithmic outputs influence decisions. A respondent must be able to contest material relied upon, subject to lawful confidentiality protections; a survivor must be able to challenge an erroneous classification that restricts assistance. Meaningful explanation requires intelligible reasons, relevant inputs and known limitations, not necessarily indiscriminate publication of source code or intimate datasets. Judicial urgency remains compatible with these safeguards: section 23 of the PWDVA permits interim and ex parte protection on the statutory conditions.²⁴ Human oversight must preserve that protective jurisdiction without allowing a machine score to substitute for the magistrate's satisfaction.

7. Institutional Accountability and a Survivor-Centred Model

A defensible model should differentiate applications by their consequences. Informational assistance requires maintained legal sources and reliable referral pathways. Professional decision support additionally requires contextual validation, audit trails and documented review. Automated determinations of credibility, criminal liability or eligibility for urgent protection present fundamentally different concerns and should not be delegated to

probabilistic outputs. This graduated approach is proposed here as an institutional safeguard, not presented as an existing comprehensive statutory classification of domestic-violence AI.

India's AI Governance Guidelines, 2025 discuss fairness, accountability, transparency, existing legal mechanisms and voluntary risk mitigation.²⁵ Their relevance lies in providing governance principles; they do not themselves create a complete enforceable domestic-violence-specific regime. Deploying institutions should translate applicable legal duties and justified safeguards into procurement conditions, operational protocols and reviewable decisions. A designated officer should remain answerable for deployment, including changes introduced through model updates. Responsibility cannot dissolve between a vendor that disclaims legal expertise and an authority that treats vendor assurances as sufficient diligence.

Accountability should follow actual functions. A developer may control training, testing and warnings; an institution may control lawful data access, deployment purpose and staff training; an individual decision-maker may control how an output is used. A harmful result does not by itself establish the same liability for each actor: the applicable duty, breach, causation and remedy require separate examination. Contracts should preserve audit access, incident records and cooperation with investigations, without purporting to extinguish statutory obligations or affected persons' remedies. Supervisors need authority and time to reject automated recommendations.

Remedial design must also address harms occurring before judicial proceedings begin. Section 29 of the PWDVA provides an appeal against a magistrate's order, but an adverse chatbot response is not such an order.²⁶ An inaccessible interface or erroneous referral may therefore obstruct protection without producing a decision amenable to that statutory appeal. A programme needs an immediate human reconsideration channel that does not depend on the applicant identifying the correct legal theory of liability. Judicial remedies cannot substitute for basic operational correction at the point where access fails.

Survivor participation should shape contact methods, escalation rules and explanations before deployment, through ethically approved and safely conducted consultation. Research must never make access to assistance conditional on participation. Independent evaluation should compare the intervention with realistic alternatives and monitor

whether it exposes users, entrenches exclusion or increases burdens on frontline personnel. A clear complaints pathway and the capacity to suspend unsafe functions are as important as initial testing. Institutional success should be measured by safe, accountable access to protection, not the volume of personal information accumulated.

8. Conclusion

AI's contribution to addressing domestic violence in India is conditional, not self-validating. Its useful role lies in assisting people to understand remedies, organise material and reach responsible institutions. The same capabilities can intensify coercion, misclassify vulnerability and obscure the basis of consequential decisions. The doctrinal analysis reveals neither a complete regulatory vacuum nor a legal framework that automatically resolves every algorithmic risk. Domestic-violence protection, criminal procedure, privacy, electronic evidence and intermediary duties perform different functions and must be applied together without erasing their limits.

A survivor-centred approach therefore requires more than consent screens and nominal human supervision. It requires demonstrable necessity, contextual evaluation, evidentiary discipline, accountable institutional ownership and accessible alternatives. The phased data-protection regime makes accurate attention to commencement particularly important; enacted safeguards must not be mistaken for universally operative remedies. Ultimately, technology should expand the survivor's practical agency while preserving lawful adjudication. The appropriate ambition is not an automated system that claims to know who deserves protection, but an accountable system that enables qualified institutions to respond more carefully, promptly and fairly.

References

1. Protection of Women from Domestic Violence Act, 2005, s. 3.
2. Vivian Hui, Rose E. Constantino and Young Ji Lee, "Harnessing Machine Learning in Tackling Domestic Violence-An Integrative Review" (2023) 20(6) *International Journal of Environmental Research and Public Health* 4984, sections 4–6, doi:10.3390/ijerph20064984.
3. Protection of Women from Domestic Violence Act, 2005, ss. 17–23.
4. Protection of Women from Domestic Violence Act, 2005, ss. 8–10 and 12(1).
5. *Hiral P. Harsora v. Kusum Narottamdas Harsora* (2016) 10 SCC 165; Protection of Women from Domestic Violence Act, 2005, s. 2(a).

6. Bharatiya Nyaya Sanhita, 2023, ss. 78, 85–86 and 351.
7. Bharatiya Nagarik Suraksha Sanhita, 2023, s. 173(1), particularly clause (ii).
8. National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, NIST AI 600-1 (July 2024), section 2.2, doi:10.6028/NIST.AI.600-1.
9. Hui, Constantino and Lee, “Harnessing Machine Learning in Tackling Domestic Violence” (n. 2), sections 5–6.
10. Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart and Nicola Dell, “A Stalker’s Paradise’: How Intimate Partner Abusers Exploit Technology” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM 2018), paper 667, 1–13, doi:10.1145/3173574.3174241.
11. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(2)(b) and 3(3), as amended by G.S.R. 120(E), 10 February 2026, effective 20 February 2026. The qualifying-content complaint period in r. 3(2)(b) was reduced from twenty-four hours to two hours.
12. Bobby Chesney and Danielle Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security” (2019) 107 *California Law Review* 1753, discussion of the “liar’s dividend”, doi:10.15779/Z38RV0D15J.
13. Constitution of India, art. 14.
14. *K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
15. Ministry of Electronics and Information Technology, G.S.R. 843(E), 13 November 2025, clauses (a)–(c), issued under the Digital Personal Data Protection Act, 2023, s. 1(2); Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025, r. 1(2)–(4). This article distinguishes enactment from the notified dates of commencement.
16. Information Technology Act, 2000, s. 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rr. 3–8; Digital Personal Data Protection Act, 2023, s. 44(2), read with G.S.R. 843(E), 13 November 2025, clause (c), deferring commencement of the omission of s. 43A.
17. Digital Personal Data Protection Act, 2023, ss. 4–8 and 17(1)(a)–(c). Section 17(1) excepts ss. 8(1) and 8(5) from its disapplication of Chapter II. Substantive commencement remains subject to the notification cited in n. 15.
18. Digital Personal Data Protection Act, 2023, Chapter III, ss. 11–14. These provisions address access to information, correction and erasure, grievance redressal and nomination, rather than a general right against solely automated decision-making.
19. Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63 and Schedule. Section 170(2) preserves the former Evidence Act for proceedings and investigations specified in the saving clause that were pending immediately before commencement.
20. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1; Indian Evidence Act, 1872, s. 65B.
21. Bharatiya Sakshya Adhiniyam, 2023, s. 170(2).
22. Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86 (August 2006), sections 3.1.2 and 4.2.2, doi:10.6028/NIST.SP.800-86. This source concerns forensic integrity, not Indian admissibility rules.
23. *Vibhor Garg v. Neha*, 2025 INSC 829 (14 July 2025), paras. 10–10.1, 12.6 and 13; Indian Evidence Act, 1872, s. 122; Family Courts Act, 1984, s. 14.
24. Protection of Women from Domestic Violence Act, 2005, s. 23, read with s. 16 concerning in camera proceedings.
25. Ministry of Electronics and Information Technology, *India AI Governance Guidelines* (November 2025), parts 1, 2 and 4, particularly the discussions of voluntary frameworks, accountability mechanisms and liability.
26. Protection of Women from Domestic Violence Act, 2005, s. 29. The distinction between appellate review of judicial orders and operational reconsideration of software outputs is the analysis advanced here.

Disclaimer/Publisher’s Note: The views, findings, conclusions, and opinions expressed in articles published in this journal are exclusively those of the individual author(s) and contributor(s). The publisher and/or editorial team neither endorse nor necessarily share these viewpoints. The publisher and/or editors assume no responsibility or liability for any damage, harm, loss, or injury, whether personal or otherwise, that might occur from the use, interpretation, or reliance upon the information, methods, instructions, or products discussed in the journal’s content.
