

# INDIAN JOURNAL OF LEGAL REVIEW

INSTITUTE OF LEGAL EDUCATION

# INDIAN JOURNAL OF LEGAL REVIEW

**APIS: 3920-0001 | ISSN: 2583-2344 | Impact Factor: 7.58**

*(Open Access Peer-Reviewed Refereed Academic Journal - Institute of Legal Education)*

**Volume 6 | Issue 12 | Year 2026** **Article #6 | Pages 62 - 75 | Date: 15 Nov 2026**


PUBLISHED ARTICLE BIBLIOGRAPHIC & VERIFICATION RECORD

# AI-Facilitated Economic Abuse in Intimate Relationships: Legal Protection and Remedies in India


Authors: Rishika Pandey (Chandigarh University); Dr. Maya Devi (Chandigarh University)



*Keywords: economic abuse; artificial intelligence; intimate relationships; domestic violence; digital evidence; financial autonomy.*

**Recommended Citation (OSCOLA Format)**

Rishika Pandey, Dr. Maya Devi, "AI-Facilitated Economic Abuse in Intimate Relationships: Legal Protection and Remedies in India" (2026) 6(12) INDIAN JOURNAL OF LEGAL REVIEW 62 - 75; AIT: IJLR/XRHT-0015; Available at: https://ijlr.iledu.in/IJLR/XRHT-0015



Open Access - Creative Commons Attribution 4.0 (CC BY 4.0) | https://creativecommons.org/licenses/by/4.0/



**JOURNAL & ISSUE LINKS**

**Journal's Home Page –** https://ijlr.iledu.in/

**Journal's Editorial Page –** https://ijlr.iledu.in/editorial-board/

**Volume 6 and Issue 12 of 2026 (Access Full Issue on –** https://ijlr.iledu.in/category/volume-6-and-issue-12

**AIT Sovereign Verification Link –** https://ijlr.iledu.in/IJLR/XRHT-0015

**ARTICLE IDENTIFICATION TAG**

**AIT: IJLR/XRHT-0015**

**About AIT Verification:**
AIT (Article Identification Tag) is ILE's sovereign identifier. Scan QR or visit link for live article verification & certificates.

**PUBLISHER INFORMATION & COPYRIGHT DISCLAIMER**

**Publisher: Prasanna S, Chairman of Institute of Legal Education**

No. 08, Arul Nagar, Seera Thoppu, Maudhanda Kurichi, Srirangam, Tiruchirappalli - 620102

Phone: +91 73059 14348 | Email: info@iledu.in / Chairman@iledu.in



**(c) Institute of Legal Education - Copyright Disclaimer:**

All rights are reserved with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For full details refer https://ijlr.iledu.in/terms-and-condition/.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# AI-FACILITATED ECONOMIC ABUSE IN INTIMATE RELATIONSHIPS: LEGAL PROTECTION AND REMEDIES IN INDIA

**AUTHOR –** RISHIKA PANDEY* & DR. MAYA DEVI**

* LLM STUDENT, UNIVERSITY OF LEGAL STUDIES, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA.

** ASSISTANT PROFESSOR, UNIVERSITY OF LEGAL STUDIES, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA.

**BEST CITATION –** RISHIKA PANDEY & DR. MAYA DEVI, AI-FACILITATED ECONOMIC ABUSE IN INTIMATE RELATIONSHIPS: LEGAL PROTECTION AND REMEDIES IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (12) OF 2026, PG. 62-75, APIS – 3920 – 0001 & ISSN - 2583-2344.

**Abstract**

Economic abuse can leave a woman with an income on paper but little control over how she earns, spends or saves it. Artificial intelligence may assist an intimate partner in maintaining that control through impersonation, synthetic threats or the analysis of personal financial information. Indian law already recognises economic abuse, yet recognition does not settle who can obtain protection, how the conduct can be proved or which order will prevent` further loss. This paper examines those questions through doctrinal analysis of Indian legislation and judgments, supported by research on economic and technological abuse. A limited comparison with England and Wales helps assess possible reforms. The paper argues that the immediate difficulty is the uneven availability and practical use of existing remedies. It distinguishes AI-assisted conduct from ordinary misuse of digital accounts and separates proof of a record from proof of responsibility for it. Its contribution is a structured inquiry connecting the qualifying relationship, the economic interference, the available evidence and the relief sought. Targeted procedural guidance, proportionate preservation of records and effective interim orders offer a defensible response. Any wider statutory reform should address an identified gap and preserve safeguards against unsupported allegations. The analysis distinguishes current law from provisions awaiting commencement as at 14 November 2026.

***Keywords:*** *economic abuse; artificial intelligence; intimate relationships; domestic violence; digital evidence; financial autonomy.*

## I. Introduction

A woman may be able to open a banking application and still be unable to decide what happens to her money. Her partner may require explanations for each payment, interfere with her work or use threats to obtain transfers. Where the relationship is covered by the Protection of Women from Domestic Violence Act, 2005, such conduct can already fall within economic abuse. The legal question becomes harder when the partner uses an AI-generated message or synthetic recording, or uses an AI service to

interpret information obtained from her accounts. The means of control may change while the financial dependency remains familiar.[132]

Treating this problem as a complete absence of law would overlook the breadth of the 2005 Act. Treating it as an ordinary financial dispute would overlook the relationship in which the conduct occurs. Economic abuse research connects control over resources with restrictions on a survivor's capacity to live independently. Technology research adds that access gained through an intimate relationship can be used against the person who originally shared it. Neither finding establishes that every disagreement over household expenditure is abuse. Both require the decision-maker to examine the purpose, circumstances and consequences of the interference.[133,134]

This paper asks whether Indian law provides effective protection when AI facilitates economic abuse against women in intimate relationships. It examines the limits of the domestic relationship requirement, the relationship between protective and criminal remedies, and difficulties in obtaining reliable electronic evidence. The central argument is that the strongest immediate response lies in connecting existing substantive protection with usable procedures. An additional offence would require a separate justification. The mere involvement of AI cannot supply the elements missing from an existing offence or relieve a claimant of proving responsibility.

The method is doctrinal. The paper interprets legislation and judgments and tests their application through clearly hypothetical situations. The law of England and Wales provides a limited comparison because it expressly addresses economic abuse and controlling behaviour. The study draws on published materials and does not collect field data. Foreign research supports particular propositions about economic and technological abuse, but cannot establish the frequency of AI-assisted abuse in India. The structured inquiry developed in section VII brings the analysis together by examining how the relationship, the economic harm, the proof and the proposed relief fit within a concrete claim.

## II. Understanding AI facilitated economic abuse

Economic abuse extends beyond taking money from an account. Adams and her co-authors developed a scale addressing conduct that controls or exploits economic resources. Later research has also examined interference with employment and the resulting loss of economic self-sufficiency. These distinctions matter legally. A partner may prevent independent earning without acquiring money personally, or impose debt that continues to restrict the survivor after separation. The harm is therefore not exhausted by the value of a disputed transaction.[135,136,137]

Stark's account of coercive control helps explain why apparently small restrictions can acquire significance within a relationship. Repeated supervision of spending may make ordinary decisions dependent on permission. A woman who expects retaliation for paying for transport or legal advice may avoid those expenses even when the account remains in her name. The multicountry review by Postmus and others nevertheless cautions against assuming a single settled definition or

[132] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), s. 3, Explanation I(iv).
[133] Judy L. Postmus, Sara Beth Plummer, *et al.*, "Understanding Economic Abuse in the Lives of Survivors" 27 *Journal of Interpersonal Violence* 411–430 (2012).
[134] Diana Freed, Jackeline Palmer, *et al.*, "A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology" in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Paper 667, 1–13 (ACM, New York, 2018), DOI: 10.1145/3173574.3174241.
[135] Adrienne E. Adams, Cris M. Sullivan, *et al.*, "Development of the Scale of Economic Abuse" 14 *Violence Against Women* 563–588 (2008).
[136] Postmus and Plummer, *supra* note 2.
[137] Angela Littwin, "Coerced Debt: The Role of Consumer Credit in Domestic Violence" 100 *California Law Review* 951–1026 (2012).

measurement of economic abuse. For Indian legal analysis, the statutory language and the facts must remain the starting point.[138,139]

The AI element needs an equally careful boundary. Changing a password, tracking a transfer or sending an abusive message does not, by itself, establish AI use. The term is used here where a system generates or materially transforms content, infers information from data or assists a decision in a way relevant to the alleged control. A complaint should identify that contribution where the evidence allows. If AI involvement remains uncertain, the underlying interference can still be examined under ordinary law. Protection should not depend on the survivor correctly naming a model or explaining its internal operation.

Bellini's research describes how intimate partners use technology to exploit, monitor, restrict and sabotage financial resources. Freed and others explain how familiarity with a survivor's devices and routines can assist technological abuse. These studies support attention to access and relationship context. They do not establish that the conduct studied necessarily involved AI. The distinction is essential if the present subject is to have a defensible research basis rather than become a new label for every digital financial harm.[140,141]

The AI-specific study by Kim, Ristenpart and Dell provides a narrower foundation. Their experimental scenarios explored whether conversational AI could facilitate coercive control and identified weaknesses in responses to abusive interactions. It was an experimental investigation, not a representative study of actual Indian relationships. Its relevance is that the possibility of assistance extends beyond a single synthetic image. The legal significance of any resulting conduct still depends on what the person did, the effect on the survivor and the applicable rule.[142]

Consider two hypothetical situations. In the first, a partner uses a fabricated recording to threaten a woman into transferring savings. In the second, a partner uses AI-generated communications to interfere with her small business and make her dependent on household money. The first may raise questions of intimidation, extortion or personation. The second may involve economic abuse even where no money reaches the partner. Research on deep fakes supports concern about fabricated material being used for intimidation and sabotage. These examples illustrate possible legal applications; they are not reported findings about particular Indian cases.[143]

## III. Protection under the Indian legal framework

### *Domestic violence protection and its boundaries*

The 2005 Act requires attention to who is entitled to invoke it. A domestic relationship under section 2(f) is a statutory category involving the relationships and shared household connection described there. Marriage and a qualifying relationship in the nature of marriage are relevant, but the broad social

[138] Evan Stark, *Coercive Control: The Entrapment of Women in Personal Life* (Oxford University Press, New York, 2007).
[139] Judy L. Postmus, Gretchen L. Hoge, *et al.*, "Economic Abuse as an Invisible Form of Domestic Violence: A Multicountry Review" 21 *Trauma, Violence, & Abuse* 261–283 (2020).
[140] Rosanna Bellini, "Paying the Price: When Intimate Partners Use Technology for Financial Harm" in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Article 872, 1–17 (ACM, New York, 2023), DOI: 10.1145/3544548.3581101.
[141] Freed and Palmer, *supra* note 3.
[142] Haesoo Kim, Thomas Ristenpart, *et al.*, "AI-Facilitated Coercive Control: An Experimental Study" in *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, 1–16 (ACM, New York, 2026), DOI: 10.1145/3772318.3790859.
[143] Robert Chesney and Danielle K. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 *California Law Review* 1753 (2019).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

expression "intimate relationship" cannot replace that legal inquiry. A dating relationship conducted entirely online does not automatically satisfy the provision. Equally, physical separation at the time of the complaint does not automatically defeat protection. The facts establishing the relationship must be examined before the technology is considered.[144]

In *Prabha Tyagi v. Kamlesh Devi*, the Supreme Court rejected restrictive approaches to access under the Act and explained the significance of a woman's right to reside in a shared household.[145] Its reasoning prevents current residence from becoming a mechanical condition that excludes a woman already driven away. It does not remove every statutory relationship requirement. In *Hiral P. Harsora v. Kusum Narottamdas Harsora*, the Court struck down the words "adult male" in the definition of respondent.[146] The category therefore extends beyond an adult male partner where the other statutory conditions are met.

Section 3 recognises deprivation of resources, disposal of property and restrictions on access within its definition of economic abuse. Its application turns on the interference and the woman's entitlement or need, rather than on whether the respondent acted through paper records or an application. This permits a reasoned argument that AI-assisted restrictions may fall within existing protection. It does not mean that a consensual household budget, a genuine inability to pay or every disputed transaction satisfies the provision. Evidence of coercion, deprivation and the overall circumstances must explain why the conduct is abusive.[147]

The property and residence decisions offer useful, limited analogies. *Krishna Bhattacharjee v. Sarathi Choudhury* recognised the continuing deprivation associated with withholding stridhan in the circumstances before the Court.[148] *Satish Chander Ahuja v. Sneha Ahuja* rejected an unduly narrow understanding of the shared household.[149] Neither judgment decided AI-assisted abuse. Their relevance lies in treating continued control over resources and access to housing as matters requiring substantive protection. The decisions support an analogy with continued digital exclusion, although applying that reasoning to AI-assisted interference requires a further legal argument.

The Act also supplies a range of responses. Protection orders under section 18 can address specified interference, including dealings with assets within the statutory terms. Monetary relief under section 20 may address losses and maintenance. Section 22 provides for compensation and damages for the injuries described there, while section 23 permits interim and, where its conditions are met, ex parte orders. These powers offer a starting point for a carefully framed application concerning AI-assisted control. Relief must remain within the court's jurisdiction and should specify the conduct to be restrained and the financial interest to be protected.[150]

***Criminal offences and misuse of computer resources***

Protective relief and criminal conviction answer different questions. Sections 85 and 86 of the Bharatiya Nyaya Sanhita, 2023 address cruelty by a husband or his relative within the definition

[144] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), ss. 2(a), 2(f) and 2(s).
[145] (2022) 8 SCC 90.
[146] (2016) 10 SCC 165.
[147] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), s. 3, Explanation I(iv) and Explanation II.
[148] (2016) 2 SCC 705.
[149] (2021) 1 SCC 414.
[150] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), ss. 18, 20, 22 and 23.

Parliament enacted. Serious economic conduct may satisfy that definition on appropriate facts, but economic abuse under the 2005 Act is not automatically cruelty under the criminal provision. The relationship restriction and the required nature of the conduct must be established. Extending the word "cruelty" through general references to technological harm would conceal rather than resolve those requirements.[151]

Other offences may apply without that marital connection. A fabricated threat used to dishonestly induce delivery of property can require examination under section 308 on extortion. Deceptive inducement and personation may engage sections 318 and 319. A threat intended to cause alarm or compel conduct must be considered against section 351. The fact that an image or voice is synthetic does not determine the answer. The prosecution must prove the relevant threat or deception, the accused's participation and the other elements of the particular offence. A failed attempt to obtain money and a completed transfer also require separate legal treatment.[152]

The Information Technology Act, 2000 addresses unauthorised interference with computer resources and particular forms of identity misuse. Section 43 concerns specified acts involving access, copying, disruption or alteration without permission; section 66 attaches criminal consequences where the prescribed dishonesty or fraud is present. Sections 66C and 66D address specified identity theft and cheating by personation through computer resources. Shared access within a relationship makes permission fact-sensitive. Earlier consent to help with banking cannot simply be assumed to authorise every later act, although proving that the accused exceeded the permission remains necessary.[153]

These provisions leave room for protection, but they distribute responsibility across several legal inquiries. A woman may establish that her partner restricted essential expenditure while finding it difficult to show an unauthorised computer act or the ingredients of a specific offence. Conversely, electronic personation may be prosecutable even when the relationship does not qualify under the domestic violence legislation. This uneven coverage explains why the paper separates a gap in eligibility, a failure of proof and a failure to enforce an available remedy. Each calls for a different response.

The economic consequence alone cannot determine criminal responsibility. A loss may result from a payment error, an independent fraudster or an inaccurate recommendation accepted without coercion. Even a partner's involvement in choosing a financial tool does not establish a dishonest purpose. An investigation should examine those explanations against the available records. This is particularly important where the accusation rests on a persuasive synthetic recording: the apparent speaker, the person who created the file and the person who used it to obtain money may be different people. The relevant offence must be attributed to the accused on evidence, rather than inferred from financial loss within an unhappy relationship.

***Maintenance and financial disclosure***

Section 144 of the Bharatiya Nagarik Suraksha Sanhita, 2023 provides a maintenance route subject to its own conditions, including those governing a wife's claim. It cannot be presented as a general

[151] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 85 and 86.
[152] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 308, 318, 319 and 351.
[153] The Information Technology Act, 2000 (Act 21 of 2000), ss. 43, 66, 66C and 66D.

compensation provision for every intimate partner. Where applicable, however, it may matter to a woman whose access to earnings or household support has been obstructed. A claim for ongoing support and a claim for loss caused by a particular deceptive transaction serve different purposes. The appropriate statutory route should follow the relief actually needed.[154]

In *Rajnesh v. Neha*, the Supreme Court addressed financial disclosure, assessment of maintenance and overlapping claims. Accurate disclosure becomes especially important where an apparently convincing digital document misstates income or liabilities. The judgment supplies principles concerning maintenance proceedings; it does not itself establish the truth of a contested electronic statement. Independent records and an opportunity to challenge the material remain necessary. Coordination of proceedings should also prevent an award under one route from being hidden while recovery for the same financial need is sought under another.[155]

### IV. Privacy consent and financial autonomy

Financial control often depends on access to information before it produces a visible loss. The ability to monitor appointments, earnings or payments can reveal a plan to obtain employment or seek legal help. *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognises privacy in connection with dignity and personal autonomy. Read alongside constitutional equality, that reasoning supplies a basis for evaluating laws and institutional responses that leave women unable to exercise ordinary financial choices. It should not be converted into an assertion that every private dispute creates direct constitutional damages claim against the partner.[156,157]

Consent requires attention to the particular act and its circumstances. A woman may share credentials for a payment while refusing ongoing surveillance or the use of her records to pressure her into leaving work. A joint account can involve genuine common management, coercive dependency or a mixture that changes over time. The distinction cannot be resolved from account ownership alone. Research on digital coercive control is helpful because it examines how access, proximity and expectations within relationships affect the meaning of technological conduct. Legal responsibility must still be tied to the rule being invoked.[158]

The Digital Personal Data Protection Act, 2023 requires particular care about time. As at 14 November 2026, its main processing obligations and individual rights remain scheduled for commencement eighteen months from 13 November 2025, rather than being generally available remedies already in force. The official consolidated Act records that staged commencement. The 2025 Rules also distinguish between provisions commencing on publication, after one year and after eighteen months. The following discussion therefore considers the enacted framework and its limits, without treating all of it as an immediately usable complaint mechanism.[159,160]

[154] The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), ss. 144–147.
[155] (2021) 2 SCC 324.
[156] (2017) 10 SCC 1.
[157] The Constitution of India, arts. 14, 15 and 21.
[158] Bridget A. Harris and Delanie Woodlock, "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies" 59 *The British Journal of Criminology* 530–550 (2019).
[159] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 1(2), commencement annotation to the official consolidated text.
[160] The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), dated Nov. 13, 2025, r. 1.

Section 3(c)(i) of the enacted Act excludes personal data processed by an individual for a personal or domestic purpose. Its application to disputed abusive conduct requires interpretation; the existence of a relationship should not be treated as a conclusive answer in every case. A platform's own processing also raises a different question from an individual partner's conduct. Even where the framework applies after commencement, its penalty structure must not be confused with an automatic right to financial compensation for the survivor. These limits support retaining domestic violence relief and other appropriate proceedings as distinct routes.[161]

An additional difficulty concerns what the survivor is asking to happen to her information. Removal of a threatening synthetic file may reduce ongoing harm, while immediate destruction of every related record could obstruct proof of its origin and use. A request to preserve evidence and a request to restrict further circulation should therefore be considered separately. Any preservation arrangement should identify the relevant material, limit access and provide an appropriate duration. This is a proposed safeguard for reconciling privacy with proof, rather than a claim that the DPDP Act itself supplies every necessary order in a domestic violence proceeding.

## V. Digital evidence attribution and access to justice

### *What an electronic record can establish*

An electronic record can be genuine without proving the proposition for which it is offered. A bank statement may accurately show a transfer while leaving consent or coercion unresolved. A saved message may accurately record a threat to release a fabricated image even though the image falsely depicts the woman. In the latter situation, proving that the image is synthetic would not by itself disprove the threat. The court must identify whether the issue is the creation of the material, its communication, the alleged demand or the resulting restriction on financial choice. Otherwise, the debate about AI can distract attention from the act that requires proof.[162]

Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023 provide the statutory starting point for electronic records. Section 63 regulates the admission of the computer output described there and prescribes a certificate with specified information. The statutory form includes details relevant to the source and integrity of the output. Compliance with an evidentiary route does not make every assertion within the record true, or establish who acted through a device. Admissibility, authenticity, authorship and the weight of the material require attention to their different purposes.[163]

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court explained the certificate requirement under the predecessor evidence legislation and the position of a litigant who lacks control of the relevant device or records. Its reasoning remains useful when considering the practical difficulty of obtaining third-party evidence. The case did not interpret the 2023 Act. Its treatment of original records, computer output and court assistance must therefore be read alongside the new wording and prescribed certificate, rather than repeated as if the legislation were unchanged.[164]

[161] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 3(c)(i), 33 and 34.
[162] Chesney and Citron, *supra* note 12.
[163] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 61–63 and sch.
[164] (2020) 7 SCC 1.

The difficulty is often access to the material needed for that process. A survivor may possess a screenshot but have no control over the service holding the original conversation. The partner may control the device, recovery address or financial correspondence. Rogers and others identify evidentiary and professional-response difficulties within the wider research on technology-facilitated abuse. A legal system that formally accepts electronic evidence can still be inaccessible if the person seeking protection cannot obtain the records necessary to present it properly.[165]

***Connecting the conduct to a responsible person***

Responsibility cannot be inferred solely from the existence of an AI-generated file. Several people may have access to an account, a device may be shared and an apparent sender may have been impersonated. The financial destination, communications surrounding a demand, control of relevant accounts and independent records may together support attribution. Each item has limits. An address associated with a household or proof that a respondent could use an AI service is insufficient by itself. The standard required for a criminal conviction must not be displaced by a general concern that AI makes fabrication possible.

Record preservation should therefore be directed towards the disputed event. Relevant transaction identifiers, dated messages, account-access information and records of the request may assist a court without requiring unrestricted disclosure of a survivor's private life. In an appropriate criminal proceeding, section 94 of the BNSS provides a route for requiring production of relevant documents or things, including the electronic material described in the provision. Its use depends on the competent authority and the procedural conditions. The immediate practical issue is often obtaining a lawful, specific request before routine deletion or loss of access defeats the inquiry.[166]

Technical assistance also needs a defined purpose. A hash can help show that a collected file has remained unchanged after collection; it does not prove that its contents were truthful when created. An expert opinion on a synthetic recording must address the material actually examined, the method and its limitations. The possibility of manipulation should neither lead to automatic acceptance of a convenient expert label nor make all electronic records suspect. The structure of section 63 and its certificate supports attention to identifiable sources and production processes instead of confidence based only on appearance.[167]

Access to justice includes the ability to seek protection while those questions are investigated. An application for interim relief under section 23 of the 2005 Act has a different purpose from a completed criminal prosecution. The court must consider the applicable statutory conditions and the available material, explain the order and permit a timely challenge. It should not require the survivor to resolve every technical dispute before considering an immediate threat to essential resources. International work on technology-facilitated violence supports examining the connection between online conduct

[165] Michaela M. Rogers, Colleen Fisher, *et al.*, "Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review" 24 *Trauma, Violence, & Abuse* 2210–2226 (2023).
[166] The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s. 94.
[167] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63 and sch.

and its effects on safety and participation, rather than confining the inquiry to the digital object alone.[168,169]

## VI. Lessons from England and Wales

The Domestic Abuse Act 2021 offers a useful comparison because its definition expressly includes economic abuse. Section 1(4) concerns behaviour adversely affecting the ability to acquire, use or maintain money or other property, or obtain goods or services. Both parties must be aged sixteen or over, and section 2 defines the required personal connection. These statutory conditions differ from the Indian scheme. In particular, the comparison draws attention to abuse between qualifying current or former intimate partners without treating cohabitation as a universal requirement. It cannot simply be imported into the Indian Act without a legislative decision about scope.[170]

Section 76 of the Serious Crime Act 2015 separately addresses controlling or coercive behaviour. It requires repeated or continuous behaviour, the specified connection and serious effect, together with the prescribed knowledge requirement. Its current scope reflects amendments addressing post-separation conduct. The point for India is the need to specify the conditions of liability if a new offence is proposed. Recognition of economic abuse in a general definition does not dispense with the elements of a particular criminal offence or make every restrictive financial decision criminal.[171]

The Home Office guidance explains economic and technological conduct within the wider pattern of control and discusses evidence relevant to investigation. That practical connection is valuable. A transaction may appear voluntary until communications, dependency and threatened consequences are examined together. Guidance can help investigators ask appropriate questions without directing them to presume guilt. The English material is persuasive comparative material for this paper; it does not create obligations for Indian courts, police officers, banks or service providers.[172]

India can learn from this approach while retaining a separate evaluation of its own remedies. Guidance on recognising digitally mediated economic restrictions can be developed within existing institutions. Expanding statutory eligibility or creating new powers against third parties would require attention to the legal basis for those changes. The differences among the jurisdictions reviewed by Postmus and others also caution against assuming that one legal model will produce the same result elsewhere. A useful reform must explain which Indian difficulty it addresses and how an affected woman will be able to use it.[173]

## VII. Strengthening protection and remedies in India

### *A structured inquiry for claims involving AI*

The preceding analysis supports four questions for organising a claim. This is an analytical proposal, not a test already laid down by an Indian court. The first question concerns the qualifying relationship and the jurisdiction in which relief is sought. Where the 2005 Act applies, the application should explain

[168] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), s. 23.
[169] UN Human Rights Council, *Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective*, UN Doc. A/HRC/38/47 (June 18, 2018).
[170] The Domestic Abuse Act, 2021 (UK Public General Acts, c. 17), ss. 1 and 2.
[171] The Serious Crime Act, 2015 (UK Public General Acts, c. 9), s. 76.
[172] Home Office, Government of the United Kingdom, "Controlling or Coercive Behaviour: Statutory Guidance Framework" (Apr. 5, 2023).
[173] Postmus and Hoge, *supra* note 8.

the domestic relationship and household connection. Where those conditions are absent, the inquiry should move to the particular offence or other available proceeding. This prevents the broad expression "AI-facilitated economic abuse" from concealing a threshold that legislation still requires.

The second question concerns the economic interest and the interference alleged. The application should identify the earning opportunity, property, payment, essential resource or access restriction involved. It should explain how the respondent's conduct affected that interest and what role AI is alleged to have played. Proof of AI use should strengthen the account of the means employed, where relevant. It should not become an additional condition that excludes conduct already covered by section 3. Equally, an assertion that a tool is intelligent should not turn an ordinary commercial loss or consensual spending arrangement into domestic abuse.[174]

The third question concerns attribution and proof. The claim should distinguish records already available from material requiring production or expert examination. A court considering an urgent order should state what the present evidence establishes and what remains disputed. A later criminal prosecution must satisfy its own requirements of proof. A respondent should be able to contest the alleged account control, communications and financial consequences through a fair procedure. The inquiry therefore resists both an automatic assumption of guilt and an automatic refusal of protection whenever a recording might have been manipulated.

The fourth question concerns the remedy and the person against whom it can lawfully operate. An order restraining a respondent's interference, a monetary award and a direction requiring production of records have different legal bases. A domestic violence order should not be described as an unrestricted power to regulate a bank or an AI provider. Where cooperation from a third party is required, the competent authority should identify the applicable power, the material sought and the opportunity for any necessary objection. The remedy must respond to the interference proved or provisionally established.[175]

The threatened-transfer hypothetical shows how this inquiry works. If the relationship qualifies, the woman may seek urgent protection by explaining the demand, the threatened consequences and the funds at risk. A prosecution for extortion would require the separate ingredients of that offence; the fabricated recording alone would not prove them. Records showing communication of the demand and the movement of money may be more important initially than identifying the precise AI model. Whether a financial institution breached an independent duty would be a separate issue requiring an appropriate legal basis and evidence.[176]

The employment-interference hypothetical produces a different emphasis. The relevant loss may be the restriction of independent earning, even if no money was transferred to the partner. Evidence must connect the respondent with the communications or interference and explain why the conduct amounts to abuse within the relationship. Any monetary claim should identify a defensible basis for the loss alleged. If the partner used a shared account, the scope of permission and its withdrawal require

[174] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), s. 3.
[175] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), ss. 18, 20, 22 and 23.
[176] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 308.

examination. Earlier lawful access should neither establish unlimited authority nor be ignored when criminal responsibility is assessed.[177,178]

A further hypothetical exposes the boundary of the proposed approach. Suppose a former dating partner, with whom the woman never shared a household and whose relationship does not otherwise qualify under the Act, uses fabricated material to obstruct her employment. The seriousness of the injury cannot by itself establish a domestic relationship. An applicable criminal provision may offer a route where its elements are met, but that does not supply the same package of protective relief. Expanding eligibility in such a situation would be a substantive legislative choice. It should be debated as a question of access to protection, with clear conditions, rather than presented as an interpretation already settled by the cases discussed here.

***Procedural reform and practical safeguards***

Practice directions and professional training should help applicants describe the conduct in ordinary language. A complaint need not begin with a technical claim that the victim cannot substantiate. It can identify who controlled access, what changed, which demand was made and what resource was lost or restricted. Where AI involvement is suspected, the record should distinguish suspicion from an observed fact. Institutional research on technology-facilitated violence highlights inconsistent definitions and gaps in evidence collection. Clear descriptions would improve the quality of both individual proceedings and future research without manufacturing certainty.[179]

Interim orders should address the financial need while controlling the risk of overreach. A restriction on further interference with a specified account may be more workable than an indiscriminate freeze of every household asset. The court should account for legitimate access, dependants and essential payments, and provide for review. Monetary relief should be linked to the losses or needs recognised by the relevant provision. A general direction to stop using AI would give little guidance about compliance and could leave the actual coercion untouched. Orders framed around identified conduct are easier to explain and enforce.[180]

Preservation and disclosure should also be proportionate. Requests should identify relevant accounts, events and periods, with protection for unrelated personal information. Survivors need routes to obtain independent financial records without relying entirely on a partner who controls the original device. Banks and digital services should develop accessible procedures for reporting impersonation and disputed control. Where a proposal would impose a new retention, disclosure or account-management duty, its legal basis must be supplied through the appropriate regulatory or legislative process. The present paper does not assume that all such duties already exist.[181,182]

These procedures should not depend on a woman obtaining the respondent's agreement to the very request intended to protect her. At the same time, an untested allegation should not justify permanent exclusion of another lawful account holder. A workable process would record the complaint,

[177] Postmus and Plummer, *supra* note 2.
[178] The Information Technology Act, 2000 (Act 21 of 2000), ss. 43 and 66.
[179] UN Women and World Health Organization, "Technology-Facilitated Violence against Women: Taking Stock of Evidence and Data Collection" (March 2023).
[180] The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), ss. 18, 20 and 23.
[181] Molly Dragiewicz, Jean Burgess, *et al.*, "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms" 18 *Feminist Media Studies* 609–625 (2018).
[182] Bellini, *supra* note 9.

identify any urgent protective step within existing authority, preserve relevant material and provide a route for review. For an AI provider, proportionate measures might include a way to report impersonation and secure relevant account records when lawfully required. These are institutional design proposals whose effectiveness and cost would need evaluation. They do not warrant routine surveillance of private conversations in the name of detecting abuse.

There remains a possible case for substantive reform where relationship eligibility or a serious pattern of conduct falls outside available protection. That case should be demonstrated through the precise gap, rather than inferred from the novelty of AI. Wider criminalisation would need clear elements, an appropriate mental requirement and safeguards for ordinary disagreements and unsupported allegations. The immediate priority supported by this analysis is a usable connection between protection, evidence and enforceable relief. Future field research could examine the time taken to obtain relevant records and interim financial relief, and whether those orders prevent further interference.

## VIII. Conclusion

Indian law already provides substantial protection against economic abuse where the statutory relationship requirements are met. AI-assisted conduct can fall within that protection, and particular offences may apply when their separate elements are proved. The main difficulties examined here concern eligibility, obtaining reliable evidence and securing relief before further financial dependency develops.

The proposed inquiry connects those issues to a remedy that the competent authority can lawfully grant. It identifies what must be proved and what may require urgent intervention. Clear complaint procedures, proportionate preservation of records and tailored interim orders could improve existing protection. Any wider legislation should address a demonstrated failure of coverage. Financial independence must be protected through a fair process that permits allegations and technical evidence to be contested.

## BIBLIOGRAPHY

### A. *Indian legislation and rules*

1. The Constitution of India.
2. The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005).
3. The Information Technology Act, 2000 (Act 21 of 2000).
4. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
5. The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).
6. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
7. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
8. The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), dated Nov. 13, 2025.

**B. *Judgments***

9. *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
10. *Krishna Bhattacharjee v. Sarathi Choudhury* (2016) 2 SCC 705.
11. *Hiral P. Harsora v. Kusum Narottamdas Harsora* (2016) 10 SCC 165.
12. *Satish Chander Ahuja v. Sneha Ahuja* (2021) 1 SCC 414.
13. *Rajnesh v. Neha* (2021) 2 SCC 324.
14. *Prabha Tyagi v. Kamlesh Devi* (2022) 8 SCC 90.
15. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

**C. *Comparative legislation***

16. The Domestic Abuse Act, 2021 (UK Public General Acts, c. 17).
17. The Serious Crime Act, 2015 (UK Public General Acts, c. 9).

**D. *Books and scholarly articles***

18. Adrienne E. Adams, Cris M. Sullivan, *et al.*, "Development of the Scale of Economic Abuse" 14 *Violence Against Women* 563–588 (2008).
19. Judy L. Postmus, Sara Beth Plummer, *et al.*, "Understanding Economic Abuse in the Lives of Survivors" 27 *Journal of Interpersonal Violence* 411–430 (2012).
20. Judy L. Postmus, Gretchen L. Hoge, *et al.*, "Economic Abuse as an Invisible Form of Domestic Violence: A Multicountry Review" 21 *Trauma, Violence, & Abuse* 261–283 (2020).
21. Angela Littwin, "Coerced Debt: The Role of Consumer Credit in Domestic Violence" 100 *California Law Review* 951–1026 (2012).
22. Evan Stark, *Coercive Control: The Entrapment of Women in Personal Life* (Oxford University Press, New York, 2007).
23. Molly Dragiewicz, Jean Burgess, *et al.*, "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms" 18 *Feminist Media Studies* 609–625 (2018).
24. Bridget A. Harris and Delanie Woodlock, "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies" 59 *The British Journal of Criminology* 530–550 (2019).
25. Diana Freed, Jackeline Palmer, *et al.*, "A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology" in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Paper 667, 1–13 (ACM, New York, 2018), DOI: 10.1145/3173574.3174241.
26. Rosanna Bellini, "Paying the Price: When Intimate Partners Use Technology for Financial Harm" in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Article 872, 1–17 (ACM, New York, 2023), DOI: 10.1145/3544548.3581101.

27. Michaela M. Rogers, Colleen Fisher, *et al.*, "Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review" 24 *Trauma, Violence, & Abuse* 2210–2226 (2023).

28. Haesoo Kim, Thomas Ristenpart, *et al.*, "AI-Facilitated Coercive Control: An Experimental Study" in *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, 1–16 (ACM, New York, 2026), DOI: 10.1145/3772318.3790859.

29. Robert Chesney and Danielle K. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 *California Law Review* 1753 (2019).

**E. *Reports and official guidance***

30. UN Women and World Health Organization, "Technology-Facilitated Violence against Women: Taking Stock of Evidence and Data Collection" (March 2023).

31. UN Human Rights Council, *Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective*, UN Doc. A/HRC/38/47 (June 18, 2018).

32. Home Office, Government of the United Kingdom, "Controlling or Coercive Behaviour: Statutory Guidance Framework" (Apr. 5, 2023).

GRASP - EDUCATE - EVOLVE