



Digital Violence against Women and the Need for Legal Reform: An Indian Perspective in the Age of Social Media and Artificial Intelligence

Dr. Surendra Kumar

Principal, Mahavir Law College Kiran Path, Mansarovar, Jaipur

Abstract

Digital technologies have expanded women's access to education, employment, political participation, financial services and public expression. The same technologies, however, are increasingly used to harass, monitor, threaten, impersonate and sexually exploit women. Digital violence includes cyberstalking, gendered abuse, doxxing, non-consensual sharing of intimate images, sextortion, account hacking, location tracking, coordinated trolling and artificial-intelligence-generated sexual deepfakes. These acts cannot be dismissed as merely "virtual" misconduct because they may produce psychological trauma, reputational damage, economic loss, social isolation and physical danger.

The present article examines digital violence against women and evaluates the adequacy of the Indian legal framework. It follows a qualitative and doctrinal research method based on the Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, Information Technology Rules and official crime statistics. The study finds that Indian law contains provisions concerning stalking, voyeurism, privacy violations, identity theft, sexually explicit material and platform grievance redressal. The Information Technology Rules were strengthened in February 2026 to regulate synthetically generated information, require labelling and provenance mechanisms and reduce the removal period for specified intimate, morphed and impersonation content to two hours.

Despite these developments, the legal framework remains fragmented. Doxxing, coordinated gendered harassment, cyber flashing, coercive digital surveillance and synthetic intimate imagery are not comprehensively addressed through clearly defined substantive offences. Victims must often rely upon several provisions enacted for different purposes. The article proposes a consent-centred definition of image-based sexual abuse, emergency civil protection orders, re-upload prevention, specialised investigative units, survivor confidentiality, platform accountability and

compensation. Legal reform must protect women without creating vague restrictions capable of suppressing legitimate expression.

Keywords: Digital violence, women, cyberstalking, intimate-image abuse, deepfakes, legal reform, intermediary liability.

1. Introduction

Digital spaces have become inseparable from contemporary social life. Education, banking, employment, political discussion, journalism, personal relationships and public services increasingly operate through mobile phones and internet platforms. For women, digital access can reduce geographical restrictions, create professional opportunities and provide spaces for collective organisation. Yet the expansion of access has not automatically removed existing gender inequalities. Social prejudices and unequal power relations have entered online environments and acquired new speed, reach and permanence.

Technology-facilitated gender-based violence has been defined as violence committed, assisted, aggravated or amplified through information and communication technologies or digital media against a person on the basis of gender. It includes sextortion, image-based abuse, doxxing, cyberbullying, sexual harassment, cyberstalking, grooming, hacking, hate speech, impersonation and the use of technology to locate or control survivors of abuse.

Digital violence differs from an isolated offensive comment. It may involve repeated conduct, sexual humiliation, exposure of private information, threats to family members, impersonation or the creation of false images intended to destroy a woman's reputation. The perpetrator may be an intimate partner, former partner, colleague, stranger, organised group or anonymous account. Automated tools make it possible to send thousands of abusive messages, create realistic sexual deepfakes or reproduce removed content across multiple services.

The distinction between online and offline violence is therefore increasingly artificial. Online threats may reveal a survivor's address, workplace or daily routine. Digital surveillance may support coercive control within an intimate relationship. A fabricated sexual image may cause expulsion from education, loss of employment, family violence or forced withdrawal from public life. Digital abuse operates through technology, but its consequences are social, economic, psychological and sometimes physical.

The problem raises a difficult legal question. The law must provide rapid and effective protection because harmful content can be copied within minutes. At the same time, regulation must remain precise and proportionate so that criticism, satire, journalism and political disagreement are not criminalised. The challenge is not to create a general right against being offended; it is to recognise identifiable forms of coercion, privacy violation, sexual exploitation and gendered intimidation.

2. Objectives of the Study

The principal objectives of the article are:

1. To explain the nature and major forms of digital violence against women.
2. To examine its psychological, social, economic and democratic consequences.

3. To analyse the relevant provisions of contemporary Indian criminal, information-technology and data-protection law.
4. To identify substantive and procedural gaps in the existing framework.
5. To examine selected international regulatory approaches.
6. To propose survivor-centred and rights-respecting legal reforms.

3. Research Methodology

The study employs a qualitative, doctrinal and analytical research method. Primary sources include the Bharatiya Nyaya Sanhita, 2023; the Information Technology Act, 2000; the Digital Personal Data Protection Act, 2023; the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as amended through 2026; and official government notifications.

The study also uses data released by the National Crime Records Bureau through the Ministry of Home Affairs and conceptual material published by the United Nations Population Fund, UN Women and the Office of the United Nations High Commissioner for Human Rights. Comparative examples have been drawn from legislation and regulatory systems in the United Kingdom, European Union and Australia. No primary survey has been conducted, and no hypothetical statistic is presented as a research finding.

4. Forms of Digital Violence against Women

4.1 Cyberstalking and digital surveillance

Cyberstalking involves repeated monitoring, contact or pursuit through electronic means. A perpetrator may continuously message a woman, follow her across platforms, monitor her online activity, track her location or create new accounts after being blocked. Technology-assisted intimate-partner abuse may also involve access to passwords, cloud accounts, cameras, shared applications or location services.

The harm lies not only in the number of messages but also in the production of continuous fear. The victim may feel that the perpetrator can reach her at any time and knows where she lives, studies or works. Digital monitoring can therefore restrict physical movement and personal autonomy.

4.2 Gendered harassment and coordinated abuse

Gendered online harassment may include sexual remarks, rape threats, death threats, misogynistic slurs, body shaming and attacks on a woman's family or character. Journalists, academics, activists, political representatives and women who express opinions publicly may face coordinated campaigns rather than isolated disagreement.

A large number of accounts can repeat the same allegation, circulate altered photographs, contact an employer and manipulate search results. The cumulative effect may force a woman to close her account or abandon professional activity. UNFPA observes that women's self-censorship in response to technology-facilitated violence silences their voices and harms democratic participation.

4.3 Doxxing and disclosure of personal information

Doxxing refers to publishing private or identifying information—such as an address, telephone number, workplace, family details or financial information—with the intention or foreseeable effect of enabling harassment or intimidation. The disclosed information may have been obtained through hacking, data brokers, public records or ordinary personal interaction.

The individual pieces of information may not always be secret. Harm arises when they are collected, contextualised and circulated to expose the victim to hostile audiences. Doxxing may convert a hostile online campaign into an immediate threat to physical safety.

4.4 Image-based sexual abuse

Image-based sexual abuse includes the non-consensual creation, distribution or threatened distribution of intimate images. An image may originally have been created without consent, shared privately with consent, or produced through manipulation. The expression “revenge pornography” is inadequate because the offence may not involve revenge and describing the material as pornography can imply voluntary participation by the victim.

Consent to the creation or private transmission of an image is not consent to its wider publication. Perpetrators may circulate intimate material after the end of a relationship, threaten publication to obtain money or sexual compliance, or repeatedly upload it after removal.

4.5 Sexual deepfakes and synthetic impersonation

Artificial-intelligence systems can create realistic images, videos and voice recordings portraying a person as engaging in conduct that never occurred. Women are particularly vulnerable to sexually explicit face-swaps, synthetic nudity and fabricated conversations. Such content can be created without any authentic intimate image of the victim.

India’s 2026 intermediary-rule amendments expressly recognise synthetically generated information, including deepfakes, voice cloning and realistic AI-altered audiovisual content. Official guidance identifies non-consensual intimate imagery, synthetic “undressing,” morphed nudity and voice-cloned sexual conversations as forms of prohibited or unlawful synthetic information.

4.6 Sextortion, impersonation and account compromise

Sextortion involves threats to release real or fabricated sexual material unless the victim provides money, further images, sexual access or some other benefit. Impersonation may involve a fake social-media profile, fraudulent dating account or altered image used to communicate in the victim’s name.

Account hacking intensifies these harms by giving perpetrators access to private messages, contacts, photographs and authentication codes. The victim may lose control over her digital identity while observers mistakenly believe that fraudulent communications are genuine.

5. Consequences of Digital Violence

Digital violence creates psychological consequences including fear, anxiety, humiliation, sleep disruption and loss of trust. A survivor may repeatedly search for copies of harmful content, avoid

social contact or become afraid to use communication technologies. The possibility that content may reappear creates continuing rather than one-time trauma.

The social consequences can be especially severe in contexts where women are held responsible for sexualised material created or distributed without their consent. A manipulated image can be treated as evidence of actual conduct. Victims may face family restrictions, broken relationships, educational interruption or workplace discrimination, while perpetrators remain anonymous.

Economic harm may arise when the victim leaves employment, changes residence, pays extortion demands or engages legal and technical assistance. Women who depend upon digital platforms for journalism, small business, teaching or creative work may lose income if abuse forces them offline.

The consequences are also political. When women withdraw from public discussion because of sexualised abuse, the apparent diversity of digital spaces becomes misleading. Formal access to a platform has limited democratic value when participation requires accepting threats and reputational destruction.

Global measurement remains difficult because definitions, survey methods and reporting practices differ. WHO reported in 2026 that an estimated 23 per cent of women worldwide had experienced digital violence, while UN institutions continue to emphasise substantial underreporting and inconsistency in measurement.

6. Extent of the Problem in India

Official crime statistics represent registered cases rather than the actual prevalence of victimisation. Many survivors may not report because of fear, shame, family pressure, lack of knowledge, distrust of authorities or the belief that anonymous perpetrators cannot be identified. NCRB data released by the Ministry of Home Affairs show that India registered 101,928 cybercrime cases in 2024, compared with 86,420 in 2023 and 65,893 in 2022. Within the 2024 classification, 1,240 cases concerned cyberstalking or cyberbullying of women and children, 601 concerned cyber blackmailing or threatening, 266 concerned fake profiles and 28 concerned defamation or morphing. These categories overlap in practice and do not capture all forms of gendered abuse.

Earlier women-specific NCRB data recorded 10,730 cybercrime cases against women in 2021, including 1,896 cases involving cyber pornography or publication of obscene sexual material, 1,172 cases of cyberstalking or cyberbullying and 276 cases of defamation or morphing. Registered cases had increased from 6,030 in 2018, although changes in awareness and reporting may also affect recorded totals.

7. Existing Indian Legal Framework

7.1 Constitutional protection of dignity and privacy

Digital violence engages the constitutional values of dignity, privacy, equality and personal liberty. Privacy includes control over personal information, bodily integrity and intimate choices.

Sexualised impersonation and non-consensual dissemination interfere not only with secrecy but with a person's ability to define her identity and participate in society.

Freedom of speech is equally relevant. The Supreme Court's invalidation of section 66A of the Information Technology Act demonstrates the constitutional danger of vague restrictions on "offensive" online expression. The official updated text of the Act records that section 66A was struck down in *Shreya Singhal v. Union of India*. Legal reform must therefore target clearly defined harm rather than undefined annoyance or offensiveness.

7.2 Bharatiya Nyaya Sanhita, 2023

Section 78 of the Bharatiya Nyaya Sanhita criminalises stalking by a man who repeatedly contacts a woman despite her indication of disinterest or monitors her use of the internet, email or another form of electronic communication. It expressly recognises electronic monitoring as stalking.

Section 77 addresses voyeurism. It criminalises watching or capturing the image of a woman engaged in a private act and disseminating such an image. Its second explanation clarifies that where a woman consents to capture but not dissemination, subsequent dissemination constitutes an offence.

Section 75 defines sexual harassment to include unwelcome sexual advances, demands for sexual favours, showing pornography against a woman's will and sexually coloured remarks. Depending upon the conduct, it may apply to online communications, although the provision is not specifically designed around platform-based abuse.

General BNS provisions relating to intimidation, extortion, cheating, forgery and defamation may also apply to digital conduct. Their use depends upon the facts, including the perpetrator's intention, the nature of the threat and whether money or another benefit was demanded.

7.3 Information Technology Act, 2000

Section 66C of the Information Technology Act criminalises fraudulent or dishonest use of another person's password, electronic signature or unique identification feature. Section 66D addresses cheating by personation through a computer resource or communication device. These provisions can apply to account takeover and certain impersonation scams.

Section 66E penalises intentionally or knowingly capturing, publishing or transmitting an image of the private area of any person without consent in circumstances violating privacy. It is gender-neutral, but its definition is limited to specified private body areas and does not comprehensively cover all manipulated intimate content or disclosure of non-visual private information.

Sections 67 and 67A address obscene and sexually explicit electronic material. Section 67A provides imprisonment and fines for publishing or transmitting material containing a sexually explicit act or conduct. Section 67B provides stronger protection concerning children.

These provisions are useful, but obscenity and privacy are not identical to non-consent. A consent-based offence should focus on the violation of sexual autonomy rather than requiring a

court to determine whether material is obscene or sexually explicit according to broader public-morality standards.

7.4 Intermediary Rules and the 2026 amendments

The Information Technology Rules impose due-diligence and grievance-redressal obligations on intermediaries. The February 2026 amendments created a specific framework for synthetically generated information. They require covered services to use reasonable technical measures to prevent unlawful synthetic content and to label permissible synthetic audiovisual content through visible notices and permanent metadata or provenance identifiers. Significant social-media intermediaries must obtain and technically verify user declarations concerning synthetic content before publication.

The amendments substantially shortened response periods. General grievances must be resolved within seven days; certain removal grievances must be handled within 36 hours; and complaints concerning specified nudity, sexual, morphed or impersonation content require removal or disablement within two hours. A complaint may be submitted by the affected person or someone acting on her behalf.

These changes recognise that delayed removal can make a remedy meaningless. Nevertheless, takedown from one platform does not necessarily prevent copies from appearing elsewhere, and private messaging, foreign services and decentralised systems present continuing enforcement problems.

7.5 Data-protection law

The Digital Personal Data Protection Act, 2023 can support protection against unauthorised processing and disclosure of personal data. However, implementation is phased. The Data Protection Board of India was formally established in November 2025, but the principal provisions governing lawful processing, consent, data-principal rights and data-fiduciary duties are scheduled to commence eighteen months after the notification of 13 November 2025. Consequently, those core provisions were not yet in force in August 2026.

Even after full commencement, data-protection law will not replace criminal and civil remedies. A malicious former partner or anonymous harasser may not operate as a conventional “data fiduciary,” and a data penalty does not necessarily provide immediate safety, removal or personal compensation.

8. Major Gaps in the Existing Framework

The first difficulty is fragmentation. A survivor may need to rely simultaneously on provisions relating to stalking, voyeurism, privacy, obscenity, identity theft, intimidation and extortion. Police officers and victims may be uncertain about the correct combination of offences, particularly where the conduct involves deepfakes, threats and repeated re-uploading.

Second, Indian criminal law does not provide a comprehensive, technology-neutral offence of image-based sexual abuse. Section 77 of the BNS is important but remains tied to the image of a woman engaged in a private act. Synthetic sexual material may depict an act that never

occurred. Section 66E is limited to images of specified private body areas, while section 67A is structured around sexually explicit material rather than consent.

Third, doxxing is not defined as a standalone offence. General provisions may apply where disclosure forms part of intimidation or harassment, but the law does not clearly address the malicious aggregation and publication of personal information that exposes a woman to foreseeable violence.

Fourth, stalking under section 78 is gender-specific and primarily focuses on conduct by a man against a woman. Protection of women is necessary, but a modern law should also recognise abuse involving proxies, organised groups, automated accounts and perpetrators whose identity or gender is unknown.

Fifth, legal remedies remain excessively criminal-law centred. A survivor may urgently need an order restraining contact, requiring de-indexing, protecting her identity and preventing re-upload. A criminal investigation may take time and does not automatically provide these civil protections. Sixth, platform removal is often content-specific. A victim may be required to report each copy separately. Without hashing, matching and cross-platform coordination, the survivor carries the burden of continuously locating the material.

Finally, official statistics are not sufficiently disaggregated. Categories combining women and children, or combining very different forms of cybercrime, make it difficult to evaluate prevalence, investigation, prosecution, conviction, removal time and survivor outcomes.

9. Comparative Legal Approaches

The United Kingdom's Online Safety Act creates offences for intentionally sharing or threatening to share intimate images without consent. Its approach recognises the threat of publication as a distinct harm rather than waiting until the image has already been circulated.

Australia's eSafety system provides an administrative image-based-abuse removal mechanism. Between August 2018 and June 2023, the regulator sent 1,961 removal requests to services and achieved full or partial removal in 89.9 per cent of those requests. The model demonstrates the value of a specialised authority able to communicate directly with platforms rather than leaving every survivor to negotiate separately.

The European Union's Digital Services Act requires accessible notice-and-action procedures, timely and non-arbitrary decisions, explanations for moderation outcomes and avenues for appeal. Its emphasis on procedure and transparency offers safeguards both for victims and for lawful expression.

These systems cannot simply be copied because legal institutions differ. They nevertheless demonstrate useful principles: specific offences, specialised removal powers, platform transparency and accessible remedies.

10. Proposed Legal Reforms

India should adopt a comprehensive statutory definition of technology-facilitated gender-based violence. The definition should cover conduct committed, assisted or amplified through digital

technology that causes or is intended to cause sexual, psychological, economic or physical harm on the basis of gender. It should guide policy without turning every unpleasant interaction into a criminal offence.

A separate consent-centred offence of image-based sexual abuse is required. It should cover creating, sharing, threatening to share, soliciting, possessing for malicious distribution and knowingly re-sharing genuine or synthetic intimate material without consent. Consent to creation, possession or private sharing should not be treated as consent to publication. The offence should include altered images, face-swaps, synthetic nudity, voice clones and material that appears to portray the identifiable victim.

Doxxing should be defined where a person intentionally or recklessly publishes identifying information without lawful justification, knowing that the disclosure is likely to expose the victim to violence, stalking, serious harassment or substantial fear. Journalistic, legal and public-interest disclosures should remain protected.

The law should also recognise coordinated harassment. Liability should arise where individuals knowingly participate in an organised campaign involving serious threats, sexualised abuse, impersonation or publication of private information. Mere criticism, unpopular opinion and spontaneous disagreement must remain outside the offence.

Survivors should have access to emergency civil protection orders through a magistrate or specialised tribunal. Such orders could restrain further contact, prohibit distribution, direct preservation of evidence, require temporary de-indexing and protect the victim's identity. Proceedings should be available electronically and should not depend upon completion of a criminal investigation.

India should consider a specialised online-safety authority or designated independent unit with power to receive complaints, issue urgent removal notices, coordinate with foreign platforms and review compliance. Such an authority must remain subject to judicial review and transparent statutory limits.

Platforms should be required to implement safety by design. This includes easily accessible reporting, trained human review, hash-based re-upload prevention, provenance preservation, warnings before forwarding intimate content and procedures allowing trusted organisations to submit complaints for survivors. Automated moderation should be audited for errors and bias.

Police capacity also requires reform. Every cyber unit should have trained personnel capable of preserving URLs, metadata, account logs and device evidence without repeatedly requiring the victim to display intimate material. A single complaint should be routed to the correct territorial authority rather than forcing survivors to approach several police stations.

Confidentiality must be strengthened. Complaints, evidence and court records containing intimate material should have restricted access. Investigators and courts should avoid language that blames the victim for taking, storing or privately sharing an image.

Compensation should address counselling, relocation, loss of employment, technical removal assistance and legal costs. Criminal punishment alone does not repair the economic and psychological damage caused by viral distribution.

Finally, all restrictions must satisfy legality, necessity and proportionality. Statutory terms should be precise, and offences should ordinarily require intention, knowledge or recklessness. Public-interest reporting, evidence of crime, lawful investigation, medical use and bona fide artistic or academic material require carefully drafted defences.

11. Findings

The study finds that digital violence is not an entirely new category of harm but a technology-enabled transformation of stalking, sexual coercion, reputational violence and controlling behaviour. Technology changes the scale, permanence, anonymity and replicability of those acts. Indian law provides several relevant offences and has made substantial progress through the 2026 intermediary-rule amendments. The two-hour removal requirement and synthetic-content obligations respond directly to the speed of contemporary harm.

The central weakness is the absence of a coherent consent-based framework. Existing provisions focus separately on obscenity, voyeurism, private body images, impersonation and stalking. Synthetic intimate content and malicious disclosure of personal information expose the limits of these categories.

Effective reform must combine criminal law, civil protection, platform regulation, investigative capacity and survivor services. No single provision can address the full lifecycle of digital violence—from creation and threat to circulation, removal, re-upload and long-term rehabilitation.

12. Conclusion

Digital violence restricts women's autonomy in spaces that have become essential for education, livelihood, relationships and citizenship. Its seriousness cannot be measured only by whether physical contact occurs. A threat, deepfake or disclosure of personal information can reorganise a woman's entire offline life.

India's existing laws offer important protections. Cyberstalking, voyeurism, identity theft, privacy violations and sexually explicit electronic publication are punishable. The 2026 rules governing synthetic information and rapid content removal represent a significant regulatory advance. Yet survivors still face a fragmented system in which no single law clearly captures the violation of sexual consent, identity and safety produced by image-based and AI-enabled abuse.

Legal reform should therefore move from an obscenity-centred approach to a consent-, dignity- and safety-centred approach. It should provide urgent removal, protection against repetition, confidentiality, compensation and specialised investigation. At the same time, the law must avoid vague offences that could suppress criticism and lawful expression.

The objective is not to make digital spaces free from disagreement. It is to ensure that women can participate without being subjected to sexual exploitation, surveillance, intimidation and

technologically manufactured humiliation. A safe digital environment is not a special privilege for women; it is a necessary condition of equality and democratic participation.

References

Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023.

Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.

European Parliament and Council. (2022). *Regulation (EU) 2022/2065 on a Single Market for Digital Services*.

Government of Australia, eSafety Commissioner. (2024). *Image-Based Abuse Scheme: Regulatory Guidance*.

Government of India, Ministry of Electronics and Information Technology. (2026). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended*.

Government of India, Ministry of Home Affairs. (2026). *National Cyber Crime Data: Crime in India 2024*.

Information Technology Act, 2000, Act No. 21 of 2000.

Office of the United Nations High Commissioner for Human Rights. (2025). *Technology-Facilitated Gender-Based Violence*.

United Kingdom. (2023). *Online Safety Act 2023*.

United Nations Population Fund. (2023). *Measuring Technology-Facilitated Gender-Based Violence: A Discussion Paper*.

United Nations Population Fund. (2024). *Technology-Facilitated Gender-Based Violence: A Framework for Programming*.

UN Women. (2025). *Global Trends to Prevent and Respond to Technology-Facilitated Violence against Women and Girls*.

Cite this Article:

Kumar, Dr. Surendra , “Digital Violence against Women and the Need for Legal Reform: An Indian Perspective in the Age of Social Media and Artificial Intelligence” Shiksha Samvad International Open Access Peer-Reviewed & Refereed Journal of Multidisciplinary Research, ISSN: 2584-0983 (Online), Volume 03, Issue 03, Pp.363-373, March-2026. Journal URL: <https://shikshasamvad.com/>



This is an Open Access Journal / article distributed under the terms of the Creative Commons Attribution License CC BY-NC-ND 3.0) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. All rights reserved.



CERTIFICATE

of Publication

This Certificate is proudly presented to

Dr. Surendra Kumar

For publication of research paper title

**Digital Violence against Women and the Need for
Legal Reform: An Indian Perspective in the Age of
Social Media and Artificial Intelligence**

Published in 'Shiksha Samvad' Peer-Reviewed and Refereed
Research Journal and E-ISSN: 2584-0983(Online), Volume-03,
Issue-03, Month March 2026, Impact Factor-RPRI-3.89

Dr. Neeraj Yadav
Editor-In-Chief

Dr. Lohans Kumar Kalyani
Executive-chief- Editor

Note: This E-Certificate is valid with published paper and
the paper must be available online at: <https://shikshasamvad.com/>
DOI:- <https://doi.org/10.64880/shikshasamvad.v3i3.40>