

Digital Dignity and Gender Justice: Women's Rights, Technology, and Emerging Legal Challenges in India

Vandana Pawar¹, Sharmishtha Dongare²

^{1,2}Assistant. Professor, P.E.S. Modern Law College Pune

Abstract—Technological transformation has reshaped social, economic, and political life in unprecedented ways. For women, digital platforms have become spaces of empowerment, participation, and entrepreneurship, while simultaneously exposing them to novel forms of discrimination, violence, and exclusion. This chapter critically examines the intersection of women's rights and technology within the Indian legal framework, incorporating constitutional jurisprudence, statutory reforms between 2023 and 2025, and emerging judicial responses to cyber harms, artificial intelligence (AI), surveillance, and digital labour exploitation. Drawing upon domestic and international legal standards, the chapter argues that a gender-responsive techno-legal governance model is essential to protect women's digital dignity and ensure substantive equality in India's evolving digital ecosystem.

I. INTRODUCTION

The digital revolution has altered the nature of rights, responsibilities, and state regulation. Internet connectivity, artificial intelligence, data analytics, and platform economies have created new opportunities for women in education, employment, entrepreneurship, and political participation. At the same time, digital environments have become sites of harassment, exploitation, privacy invasion, and algorithmic discrimination.

Women's rights discourse can no longer be confined to physical spaces; it must extend into digital terrains where power structures are embedded within code, algorithms, and corporate governance mechanisms. The challenge lies not merely in regulating technology but in ensuring that constitutional values of equality, dignity, and autonomy permeate digital infrastructures.¹

¹ Constitution of India, arts. 14, 15, 21.

In India, where digital penetration has rapidly expanded through smartphone access and government digitisation initiatives, the intersection of women's rights and technology assumes particular significance. This chapter explores how Indian law has responded to cyber violence, data protection, AI regulation, and digital labour concerns, especially in light of legislative developments between 2023 and 2025. The constitutional promise of equality and dignity must therefore extend into cyberspace.²

II. CONSTITUTIONAL FOUNDATIONS OF DIGITAL GENDER JUSTICE

Women's rights in India are constitutionally grounded in Articles 14 (equality before law), 15 (prohibition of discrimination), and 21 (right to life and personal liberty). Judicial interpretation has expanded these guarantees to encompass dignity, privacy, and autonomy.

A landmark judgment in this regard is Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court unanimously recognised the right to privacy as a fundamental right under Article 21 (Supreme Court of India, 2017). The Court emphasised informational self-determination, bodily integrity, and autonomy—principles that directly impact women's digital rights.

The Court's reasoning in Puttaswamy provides a constitutional framework to address issues such as non-consensual image sharing, surveillance, biometric data misuse, and AI-driven profiling. Privacy is not merely secrecy but a condition for

² Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. constitution of India, art. 21.

exercising autonomy and dignity, particularly relevant for women facing digital exploitation.

At the international level, the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) obligates state parties, including India, to eliminate discrimination against women in all spheres, including technological domains (United Nations, 1979). Though drafted before the digital era, CEDAW's principles are adaptable to online contexts.

III. CYBER VIOLENCE AGAINST WOMEN: EXPANDING LEGAL RESPONSES

The core legal framework for addressing cyber violence against women in India primarily involves the Information Technology Act, 2000 (IT Act), the Indian Penal Code, 1860 (IPC), and the Protection of Children from Sexual Offences Act, 2012 (POCSO Act) where minors are involved. Constitutional provisions, particularly Article 21 (Right to Life and Personal Liberty, encompassing the right to privacy and dignity) are also fundamental.

Courts have interpreted these provisions to impose duties on government agencies, law enforcement, and online intermediaries. For instance, the Madras High Court in (*X vs. The Union of India and Ors.*) emphasized proactive blocking of Non-Consensual Intimate Imagery (NCII) under Section 69A of the IT Act and Rule 10 of the Blocking Rules, and mandated sensitive handling of complaints by law enforcement to protect victim privacy.³ Similarly, the Delhi High Court in (*'X' vs. Union of India and Ors.*) directed swift action by specialized cybercrime units (CyPAD) for content removal and protection of victim identity.⁴

3.1 Nature and Forms of Cyber Violence

Cyber violence includes cyberstalking, online harassment, doxxing, impersonation, morphing of images, revenge pornography, deepfake pornography, and gendered hate speech. Digital platforms amplify such harms due to anonymity, virality, and cross-jurisdictional complexity.

Women journalists, activists, students, and professionals frequently report coordinated trolling

campaigns aimed at silencing their voices. The psychological and reputational consequences of such abuse can be severe, often leading to self-censorship and withdrawal from public discourse.

3.2 Statutory Framework

India's primary legislation addressing cyber offences is the Information Technology Act. Section 66E penalises violation of privacy through capturing or transmitting images of private areas without consent. Section 67 and 67A criminalise publishing or transmitting obscene or sexually explicit material in electronic form.

In addition, provisions under the Indian Penal Code (now largely subsumed under the *Bharatiya Nyaya Sanhita*, 2023) address stalking, defamation, and criminal intimidation in online contexts.

However, enforcement challenges persist. Jurisdictional hurdles, lack of cyber forensic capacity, and underreporting due to stigma often hinder effective prosecution.

3.3 Judicial Interventions in Cyber Abuse Cases

Early precedent such as *Suhas Katti v. State of Tamil Nadu* (2004)⁵ marked one of India's first convictions for cyber harassment against a woman. More recently, high courts have granted injunctions in cases involving non-consensual sharing of intimate images.

In 2024–2025, Indian courts have increasingly addressed deepfake pornography and AI-manipulated images, recognising them as violations of privacy and dignity under Article 21. Courts have directed prompt takedown orders and emphasised intermediary responsibility, reflecting an evolving judicial understanding of AI-driven harms.

IV. DATA PROTECTION AND WOMEN'S INFORMATIONAL AUTONOMY

4.1 Digital Personal Data Protection Act, 2023

A significant legislative development is the Digital Personal Data Protection Act. The Act establishes a consent-based framework for processing personal data and imposes obligations on "data fiduciaries" to ensure lawful processing, security safeguards, and breach notification.

³ MANU/TN/3546/2025

⁴ MANU/DE/1477/2020

⁵ CC No. 4680 of 2004.

Although gender-neutral in language, the DPDP Act is particularly relevant for women, as data breaches often expose sensitive personal information, enabling harassment or blackmail. Consent requirements and grievance redress mechanisms under the Act may strengthen women's digital autonomy.

The 2025 Rules notified under the Act further clarify compliance obligations, including notice requirements and penalties for non-compliance (Government of India, 2025).

4.2 Surveillance and Gendered Impacts

Digital surveillance—through biometric identification systems, facial recognition, or location tracking—poses unique risks for women, especially survivors of domestic violence. The possibility of tracing a woman's digital footprint may compromise her safety.

While the DPDP Act provides a regulatory foundation, critics argue that exemptions for state agencies may weaken privacy protections. Thus, balancing national security with gender-sensitive privacy safeguards remain an ongoing challenge.

V. ARTIFICIAL INTELLIGENCE AND ALGORITHMIC BIAS

Artificial intelligence increasingly governs hiring decisions, content moderation, credit scoring, and policing. Yet AI systems trained on biased datasets risk perpetuating gender discrimination.

Recruitment algorithms have been shown globally to disadvantage women applicants when historical data reflects male dominance in certain industries (Eubanks, 2018). Content moderation systems often fail to detect gendered hate speech while disproportionately censoring women's expression.

India has initiated discussions on AI governance frameworks between 2023 and 2025, emphasising ethical AI principles. However, explicit statutory safeguards addressing algorithmic gender bias remain limited.

A gender-responsive AI regime should include:

- Mandatory algorithmic impact assessments
- Independent audits
- Transparency obligations

- Redressal mechanisms for automated discrimination

Without such measures, technological neutrality may mask structural inequality.

VI. DIGITAL LABOUR, PLATFORM ECONOMIES, AND GENDERED PRECARIETY

The growth of the digital economy has created new gig work opportunities for women in areas such as ride-sharing, content creation, remote freelancing, and e-commerce. Despite this expansion, platform-based work often does not provide essential benefits like social security, maternity protection, or equal pay. Additionally, many highly educated women remain engaged in low-productivity or part-time jobs due to societal expectations, restrictions on mobility, and a lack of flexible employment options in the formal sector. According to the PLFS 2023–24, women aged 25 and above with advanced degrees make up only 2.9% of the total employed female workforce in both rural and urban regions.⁶

Women are comparatively less inclined to enter STEM (Science, Technology, Engineering, and Mathematics) disciplines, representing 43% of total enrolment in 2021–22. This trend can be partly explained by the perception of STEM as a male-dominated field, along with factors such as care giving responsibilities, early marriage, and the high cost of higher education.⁷ Women gig workers face algorithmic monitoring and rating systems that may reproduce bias. Negative ratings, often influenced by gender stereotypes, can reduce income opportunities. Proposals such as the Right to Disconnect Bill (2025) aim to protect workers from excessive digital intrusion into personal life. Though not gender-specific, such measures may indirectly benefit women who juggle unpaid care responsibilities alongside remote work. To ensure gender justice in digital labour markets, labour law reforms must incorporate platform accountability and enforce equal remuneration principles.

⁶ Key Employment Unemployment Indicators, PLFS 2023-24 MoSPI.

⁷ Women in STEM: Challenges and Opportunities in India: IWWAGE (2024)

VII. ONLINE HARASSMENT, INTERMEDIARY LIABILITY, AND PLATFORM GOVERNANCE

Digital platforms function as intermediaries between users. Under Indian law, intermediaries enjoy conditional safe harbour protections if they exercise due diligence and comply with takedown obligations. Recent amendments to intermediary guidelines require platforms to remove unlawful content upon receiving actual knowledge or court orders. Women's rights groups have advocated for faster takedown procedures for non-consensual intimate images. Between 2023 and 2025, regulatory discussions have focused on strengthening platform accountability, including traceability requirements and grievance redressal officers. The challenge remains to balance free speech with protection against online gendered abuse.

VIII. REPRODUCTIVE TECHNOLOGIES, BIOETHICS, AND DIGITAL HEALTH

Technological advancement extends beyond cyberspace to reproductive technologies and digital health data. IVF procedures, surrogacy arrangements, and fertility tracking apps generate sensitive medical data.

Data leaks involving reproductive health information may expose women to stigma or discrimination. Thus, health data protection under the DPDP Act must be strictly enforced. Moreover, ethical regulation of reproductive technologies must prevent exploitation while safeguarding women's autonomy.

IX. CONCLUSION

Technology embodies both promise and peril. It can democratise access, amplify women's voices, and foster economic independence. Yet it can equally entrench patriarchy through digital surveillance, algorithmic bias, and cyber violence.

India's recent legislative initiatives, including the Digital Personal Data Protection Act, 2023, signal progress. Judicial pronouncements, particularly Puttaswamy, provide constitutional grounding for digital privacy and dignity. However, the rapid evolution of AI and platform economies necessitates continuous reform. Women's digital dignity must be

recognised as integral to constitutional democracy. Only through gender-responsive techno-legal governance can India ensure that digital spaces become arenas of empowerment rather than exclusion.

REFERENCES

- [1] Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.
- [2] Government of India. (2025). Digital Personal Data Protection Rules, 2025. Ministry of Electronics and Information Technology.
- [3] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- [4] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
- [5] Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India.
- [6] United Nations. (1979). Convention on the Elimination of All Forms of Discrimination Against Women.
- [7] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).