

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Synthetic Media and Gendered Harm: Balancing Free Speech and Dignity

RAJASREE R.S.*

ABSTRACT

This paper examines synthetic media and the harm it causes women in constitutional democracies. Deepfake video, AI-generated voice and synthetic avatars now spread rapidly across social media and other platforms. The law protects rights, but it struggles to balance them against free speech. The TAKE IT DOWN Act 2025 in the United States and the Digital Services Act 2022 in the European Union show legislative effort, yet enforcement remains difficult. In India, the Information Technology Act 2000, as amended in 2008, provides criminal remedies for non-consensual content, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026 now regulate synthetically generated information directly, but implementation remains slow. Decisions such as Shreya Singhal v. Union of India (2015) show the courts attempting to address harm while respecting expression. Women in politics, in the media and in the private sector face disproportionate harassment through AI-generated content, and the psychological harm, reputational damage and social silencing that follow are serious. The law permits limited restriction of speech under Article 19(2) of the Constitution of India and Article 10 of the European Convention on Human Rights while giving weight to dignity and privacy. Technology evolves faster than legal responses, so corporate responsibility and platform moderation become necessary alongside regulation, and transparency measures, consent requirements and watermarking offer further protection. The paper argues for a balanced approach in which law, ethics and social norms work together, and concludes that international cooperation and gender-sensitive policy are needed to reduce harm while maintaining free expression.

Keywords: *synthetic media, gendered harm, deepfakes, free speech, constitutional law, intermediary liability*

I. INTRODUCTION

Synthetic media plays a growing role in digital communication. It is AI-generated content, including deepfake video, synthetic voice and avatars, that imitates real persons in realistic ways. The technology allows content to be created without consent, and it spreads quickly across social media and other online platforms. Women are disproportionately targeted through

* Author is an LL.M. Graduate at Alliance School of Law, Alliance University, Bengaluru, Karnataka, India.

harassment, non-consensual sexual content and political manipulation. The harm includes psychological distress, reputational damage and social silencing, all of which affect participation in public and private life.

Constitutional democracies face a tension between freedom of expression and protection from harm. The law grants a right to free speech under Article 19(1)(a) of the Constitution of India and under the First Amendment in the United States, while imposing restrictions under Article 19(2) in India and comparable provisions elsewhere. The courts recognise the need to balance expression against dignity, as in *Shreya Singhal v. Union of India*.¹ The misuse of AI-generated content challenges the traditional understanding of defamation, privacy and obscenity.

This research analyses how legal frameworks respond to synthetic media and gendered harm. The study examines statutes including the TAKE IT DOWN Act 2025 in the United States, the Digital Services Act 2022 in the European Union, and the Information Technology Act 2000 in India as amended in 2008, together with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026. It highlights gaps in enforcement, cross-border jurisdictional difficulties and the role of corporate responsibility in platform moderation, and it offers a framework for understanding how law, ethics and social norms work together to protect women without undermining free expression.²

II. THE RISE OF SYNTHETIC MEDIA

The technological evolution of synthetic media is rapid and complex. Generative adversarial networks allow the creation of realistic images and video that imitate real persons. AI voice cloning reproduces a person's voice without consent. Realistic avatars replicate gesture and expression, which makes detection difficult.³ The technology spreads quickly online through social media and other platforms, increasing the risk of harm.⁴

The available evidence points to the disproportionate targeting of women. A 2019 report by Deeptrace, the most widely cited early survey of the field, found that 96 per cent of the deepfake videos it located online were non-consensual pornography, and that the pornographic material in its sample depicted women almost exclusively. That finding describes the position in 2019 and should not be treated as a measure of current prevalence, but it remains the reference point

¹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

² A. Mammadov, *The Rise of Deepfakes: A Deep Dive into Synthetic Media and Its Implications*, ISACA JOURNAL, vol. 1 (2025).

³ Giorgio Patrini et al., *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace, September 2019).

⁴ Rebecca Umbach, Nicola Henry, Gemma Beard & Colleen Berryessa, *Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries*, in Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (2024).

from which later work proceeds. Women in public life, in entertainment and in private spheres are most affected, and the psychological harm, reputational damage and social silencing that follow are significant and long-lasting.

Platforms and distribution channels amplify the reach and impact of synthetic content. Social media and video-sharing sites are the primary vehicles for spreading AI-generated material. The anonymity of users and the difficulty of tracing a creator complicate enforcement under existing legal provisions, and courts have recognised these challenges in cases concerning harassment and non-consensual content.

Legislative attention has followed. In the United States, the TAKE IT DOWN Act 2025 criminalises the non-consensual publication of intimate visual depictions, including computer-generated ones, and requires covered platforms to remove such material once notified. The Digital Services Act 2022 in the European Union regulates online platforms and holds intermediaries accountable for acting on illegal content. In India, the Information Technology Act 2000, as amended in 2008, penalises the capture and publication of private images and of obscene material, and the Amendment Rules 2026 add labelling and takedown duties for synthetically generated information. These frameworks show an effort to regulate the technology while respecting freedom of expression under provisions such as Article 19(1)(a) of the Constitution of India and the First Amendment in the United States.

Law, technology and corporate responsibility must therefore work together to limit gendered harm from synthetic media while respecting expression. Continuing developments require the constant monitoring and adaptation of legal frameworks.⁵

III. FORMS OF GENDERED HARM IN SYNTHETIC MEDIA

A. Non-consensual Pornography

Non-consensual pornography is the most visible form of gendered harm. Deepfake pornography disproportionately targets women and raises difficult questions under existing law. In the United States, section 230 of the Communications Decency Act limits the liability of online platforms, but state anti-revenge-pornography statutes and, since 2025, the federal TAKE IT DOWN Act provide remedies for victims.⁶ In India, section 66E of the Information Technology Act 2000, inserted by the Information Technology (Amendment) Act 2008, protects bodily privacy, while sections 67 and 67A penalise the publication and transmission of obscene and of sexually

⁵ *Deepfake AI Statistics by Fraud Data, Insights and Trends*, SCI TECH TODAY (2025).

⁶ TAKE IT DOWN Act, Pub. L. No. 119-12 (2025); Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56 (codified at 47 U.S.C. § 230); *Section 230: A Juridical History*, STANFORD TECHNOLOGY LAW REVIEW, vol. 28, no. 1 (2025).

explicit material in electronic form. The distribution of such content without consent undermines dignity and personal security.⁷

B. Harassment and Stalking

AI-generated content also facilitates harassment and stalking, and it is used for blackmail, threats and repeated intimidation. Prosecutions under state non-consensual intimate imagery statutes in the United States, and under the Information Technology Act 2000 in India, show the legal system attempting to enforce privacy and punish perpetrators while balancing free speech protections.

C. Political and Social Defamation

Political and social defamation is a further form of gendered harm. Women in public life, including politicians, journalists and activists, are increasingly targeted with synthetic content. False imagery or voice damages reputation and undermines participation in democratic processes. The law applies defamation principles, but synthetic media creates difficulties of attribution and proof.⁸

D. Psychological Impact

The psychological impact on women is serious and lasting. Victims report post-traumatic stress, reputational damage and a silencing effect. Participation in public life and in online discourse is often discouraged by the fear of AI-generated harassment. Legal remedies address tangible harm, but the emotional and social consequences require broader ethical and policy responses.⁹

IV. FREE SPEECH IN CONSTITUTIONAL DEMOCRACIES

A. Foundational Principles

The foundational principles of free speech are recognised across constitutional democracies, but they are limited in order to protect dignity and security. The First Amendment protects freedom of expression in the United States, and in *Brandenburg v. Ohio*¹⁰ the Supreme Court held that speech may be restricted only where it is directed to inciting, and is likely to produce, imminent lawless action. The Constitution of India guarantees freedom of speech and expression under Article 19(1)(a) while permitting reasonable restrictions under Article 19(2) on grounds that include decency, morality and public order. In Europe, Article 10 of the

⁷ Information Technology Act, 2000, No. 21 of 2000, §§ 66E, 67, 67A (India); §§ 66E and 67A were inserted by the Information Technology (Amendment) Act, 2008, No. 10 of 2009.

⁸ AMNESTY INTERNATIONAL, *#ToxicTwitter: Violence and Abuse against Women Online* (March 2018), <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1-1/>.

⁹ *Invisible Scars: How Deepfake Harassment Is Affecting Mental Health*, THE BRIDGE CHRONICLE (2025).

¹⁰ *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

European Convention on Human Rights balances freedom of expression against the protection of privacy and reputation. Courts interpret these provisions in the context of technology and online communication.

B. Limits of Free Speech

The recognised limits of free speech include hate speech, incitement to violence, obscenity and defamation. *R.A.V. v. City of St. Paul*¹¹ shows how a court distinguishes protected expression from punishable content, striking down a content-based ordinance while leaving the underlying conduct open to prosecution under generally applicable law. The law recognises that speech can cause tangible harm, and it imposes liability while respecting constitutional guarantees.

C. Challenges Posed by Synthetic Media

Synthetic media creates new challenges for free speech doctrine. Realistic AI-generated content blurs the line between protected expression and gendered harm. *United States v. Alvarez*¹² shows that a false statement is not for that reason alone outside constitutional protection, which illustrates the difficulty of regulating misleading or harmful AI-generated content. Courts struggle to define a clear standard for online speech without infringing the First Amendment or comparable constitutional protections elsewhere.

While free speech is essential in democratic societies, the law must evolve to address the gendered harm created by AI and synthetic media. The balance between protecting dignity and enabling expression is delicate, and it requires judicial interpretation, statutory regulation and platform accountability. The existing legal frameworks show the effort, but continued adaptation is necessary as the technology develops.

V. LEGAL AND REGULATORY RESPONSES

A. Legal Frameworks

Current legal frameworks address synthetic media and gendered harm across several jurisdictions. In the United States, the TAKE IT DOWN Act, signed into law on 19 May 2025, criminalises the non-consensual publication of intimate visual depictions, including digital forgeries, and requires covered platforms to operate a notice-and-removal process. State law adds civil remedies: section 1708.86 of the California Civil Code, introduced by Assembly Bill 602 in 2019, gives a depicted individual a cause of action against a person who creates or discloses digitally altered sexually explicit material without consent.¹³

¹¹ *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992).

¹² *United States v. Alvarez*, 567 U.S. 709 (2012).

¹³ TAKE IT DOWN Act, *supra* note 6; Cal. Civ. Code § 1708.86 (added by Assembly Bill 602, 2019).

In the European Union, the Digital Services Act 2022 regulates online platforms and requires them to act on notices of illegal content, while the General Data Protection Regulation, applicable since 25 May 2018, protects the personal data engaged by synthetic media. In India, sections 66C and 66E of the Information Technology Act 2000 address identity theft and violation of privacy, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, notified on 10 February 2026 and in force from 20 February 2026, deal directly with synthetically generated information. They require such content to be prominently labelled and to carry provenance metadata, and they shorten takedown timelines, including a two-hour window for material depicting nudity, sexual acts, impersonation, or morphed and deepfake sexual content. These instruments show an attempt to regulate the technology while protecting individual rights.¹⁴

B. Judicial Precedents

The courts show how the law is interpreted in the context of digital harm. In *Shreya Singhal v. Union of India* (2015) the Supreme Court struck down section 66A of the Information Technology Act 2000 as an unconstitutional restriction on speech, while affirming that reasonable restrictions in the interest of public order remain permissible, and it read down section 79(3)(b) so that an intermediary loses safe harbour only on receiving actual knowledge through a court order or a government notification. In *Sabu Mathew George v. Union of India* the same Court directed search engines to auto-block a list of prohibited search terms relating to pre-natal sex determination, in enforcement of section 22 of the Pre-conception and Pre-natal Diagnostic Techniques Act 1994, its principal orders being passed in 2016 and 2017. Together these decisions show the Court balancing constitutional rights against protection from harm, and they highlight the difficulty of applying older statutes to newer technology.

C. Gaps and Challenges

Significant gaps remain in the legal framework. Cross-border enforcement is difficult, and the anonymity of content creators compounds the problem. The gender-blind design of many statutes reduces their effectiveness in protecting women. The technical complexity of AI-generated content makes detection and prosecution difficult. Law, platforms and policy must interact continuously if the response is to keep pace with evolving harm while safeguarding freedom of expression.

¹⁴ Information Technology Act, *supra* note 7, §§ 66C, 66E; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (India) (notified 10 February 2026, in force from 20 February 2026).

Statutes and judicial precedent provide a structure, but continuing adaptation and coordination at the national and international levels are necessary for comprehensive protection.

VI. ETHICAL CONSIDERATIONS AND SOCIAL NORMS

A. Responsibility of Technology Companies

Technology companies hold significant responsibility for preventing gendered harm from synthetic media. Transparency about AI-generated content is necessary if real material is to be distinguished from artificial material. Watermarking allows synthetic content to be identified and helps law enforcement and victims to trace its source. Content moderation remains essential if non-consensual or harmful material is to be removed in a timely manner. A failure by platforms to act exposes users, and women in particular, to harassment and reputational damage. The Digital Services Act 2022 imposes obligations on online intermediaries to act on notices of illegal content and requires the largest platforms to assess and mitigate systemic risks, including risks of gender-based violence. United States law recognises only limited platform liability, but state-level enforcement addresses some of the harm. Corporate responsibility and compliance with statutory duties are therefore central to protecting dignity and privacy.¹⁵

B. Public Awareness

Public awareness and digital literacy play an important role in mitigating harm from synthetic media. Users must be able to recognise AI-generated content and to report harassment under the applicable statutory provisions. Awareness campaigns and education inform women about their rights under laws such as the Information Technology Act 2000 in India, section 66E of which criminalises violation of privacy. Recognising harmful content helps to reduce its psychological and reputational effects, whereas an inability to distinguish synthetic content increases vulnerability and limits participation in public life.¹⁶

C. Cultural Context

Cultural context influences the perception and the impact of synthetic media. Prevailing gender norms aggravate the social harm and contribute to victim-blaming. Marginalised women face disproportionate risks both online and offline. Societal attitudes, in combination with digital harassment, reinforce the silencing effect on women. The law provides protection, but it operates within a culture that can reduce the effectiveness of statutes and of judicial remedies.

¹⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1, arts. 16, 34.

¹⁶ Information Technology Act, *supra* note 7, § 66E.

D. Intersectionality

The intersection of gender with race, sexuality and political affiliation increases vulnerability. Women of colour, LGBTQ+ women and political activists are disproportionately affected by synthetic media. Harassment and defamation using AI-generated content undermine democratic participation and social equality. Legal frameworks address harm in general terms, but targeted attacks reveal gaps in gender-sensitive protection. The ethical responsibility of platforms and of society therefore matters alongside statutory remedies.¹⁷

Protecting women from synthetic media requires a combination of legal enforcement, corporate accountability, public awareness and cultural change. The interaction of law, ethics and social norms forms a framework for reducing harm while maintaining freedom of expression. Continuing adaptation in response to emerging technologies is what ensures that the dignity, privacy and rights of women are upheld in constitutional democracies.¹⁸

VII. BALANCING FREE SPEECH AND PROTECTION

A. Policy Strategies

Policy strategies aim to protect women from synthetic media while preserving constitutional free speech. Consent-based regulation requires that AI-generated content involving a real person be created only with clear permission. Transparency mandates, such as watermarking of AI-generated material, assist identification and tracing for enforcement purposes. Platform liability for malicious deepfakes aligns with Article 16 of the Digital Services Act, which obliges online intermediaries to operate notice-and-action mechanisms for illegal content.¹⁹

Implementing these policies requires cooperation between technology companies and law enforcement. An absence of corporate compliance increases the exposure of women to harassment and reputational damage. Statutory duties and internal platform rules work together to ensure timely intervention against harmful content.²⁰

B. The Judicial Balancing Test

Courts apply a proportionality test to weigh harm against expression. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*²¹ the Supreme Court of India held that privacy is a

¹⁷ Kimberle Crenshaw, *Demarginalizing the Intersection of Race and Sex*, 1989 UNIVERSITY OF CHICAGO LEGAL FORUM 139; Olena Hankivsky & Renee Cormier, *Intersectionality and Public Policy: Some Lessons from Existing Models*, 64 POLITICAL RESEARCH QUARTERLY 217 (2011).

¹⁸ AMNESTY INTERNATIONAL, *supra* note 8.

¹⁹ Digital Services Act, *supra* note 15, art. 16.

²⁰ AMNESTY INTERNATIONAL, *supra* note 8.

²¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

fundamental right inherent in dignity under Article 21, and that any state limitation of it must satisfy the requirements of legality, a legitimate aim and proportionality. Expression is fundamental under Article 19(1)(a), but it may be restricted under Article 19(2) to protect dignity and privacy. The proportionality approach provides a structured method for assessing the impact of synthetic media on an individual. Courts recognise that unregulated AI-generated content may cause serious psychological and social consequences for victims, and the test guides law enforcement and the judiciary in keeping any restriction on speech proportionate to the harm.²²

C. International Cooperation

International cooperation is necessary because of the cross-border nature of digital content. Harmonised laws, mutual legal assistance and the sharing of digital forensic evidence improve enforcement. The lack of uniformity across jurisdictions complicates the prosecution of creators who operate outside national boundaries. International frameworks support coordination between countries in addressing online harassment, privacy violations and defamation using synthetic media, and they help to ensure that victims have a remedy even where perpetrators operate from a foreign jurisdiction.

D. Best Practices

Best practices offer effective tools for minimising harm while maintaining free expression. The right to be forgotten, established in *Google Spain SL v. Agencia Espanola de Proteccion de Datos* in 2014, allows the removal of personal data that infringes privacy. Platform takedowns and watermarking act as preventive measures against the circulation of harmful content. Integrating technology, law and policy ensures that victims have avenues for redress while speech remains protected. These practices need continuous evaluation if they are to adapt to emerging AI tools and deepfake technologies.²³

Balancing free speech and protection therefore requires a combination of consent-based policies, judicial oversight, international coordination and proactive platform governance. The proportionality framework, statutory mandates and ethical standards together create an environment in which the dignity, privacy and rights of women are safeguarded. The evolving

²² Puttaswamy, *supra* note 21.

²³ *Google Spain SL v. Agencia Espanola de Proteccion de Datos*, Case C-131/12, ECLI:EU:C:2014:317 (CJEU, 13 May 2014); UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Practical Guide for Requesting Electronic Evidence Across Borders* (2021).

technological landscape demands constant monitoring and adaptation if the equilibrium between expression and protection in constitutional democracies is to be maintained.²⁴

VIII. RECOMMENDATIONS

- Women suffer disproportionately from synthetic media through harassment, deepfake pornography and political defamation, which affect their dignity and their participation in public life.
- Current legal frameworks address some of this harm, but they remain largely gender-blind and slow to adapt to AI technologies and online content.
- Gender-sensitive AI governance should ensure that platforms and AI tools include protective measures at the design and deployment stages.
- Multi-stakeholder cooperation between government, civil society and technology companies improves the monitoring and removal of harmful content.
- Transparency mandates such as watermarking, together with consent-based content creation, assist in tracing and regulating synthetic media for enforcement purposes.
- The judicial proportionality test guides courts in balancing free speech under Article 19(1)(a) of the Constitution of India, the First Amendment in the United States and Article 10 of the European Convention on Human Rights against the dignity and privacy of the person.
- Academic research on the intersection of AI, law and gendered impact should inform policy making and the implementation of safeguards.
- Emerging AI tools such as generative voice and text systems require continuous evaluation for harassment, defamation and wider social harm.
- Comparative study across constitutional democracies offers lessons for harmonised laws and cross-border enforcement strategies.
- The long-term social and psychological effects on women must be assessed in order to develop comprehensive and proactive interventions for safety and the protection of rights.

IX. CONCLUSION

This research shows that synthetic media causes disproportionate harm to women through harassment, deepfake pornography, political defamation and reputational damage, affecting both public and private life. The legal frameworks in India under the Information Technology

²⁴ Kate Crawford & Trevor Paglen, *Excavating AI: The Politics of Images in Machine Learning Training Sets*, 36 AI & SOCIETY 1105 (2021).

Act 2000 as amended in 2008 and the Amendment Rules 2026, in the United States under the TAKE IT DOWN Act 2025, and in the European Union under the Digital Services Act 2022, provide mechanisms to address this harm, but they remain largely gender-blind and enforcement difficulties continue.

The courts apply a proportionality test, as in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) and *Shreya Singhal v. Union of India* (2015), to balance free speech under Article 19(1) (a) of the Constitution of India, the First Amendment in the United States and Article 10 of the European Convention on Human Rights against the protection of dignity and privacy. The proportionality framework guides the judiciary and law enforcement in evaluating restrictions on harmful AI-generated content.

A combination of statutory regulation, platform accountability, ethical governance, public awareness and international cooperation forms the framework needed to reduce harm. Continuing adaptation of law, policy and technology is essential if the rights of women are to be safeguarded without undermining freedom of expression in constitutional democracies.
