SUPREMO AMICUS

VOLUME 38 | September, 2025 ISSN 2456-9704

ARTIFICIAL INTELLIGENCE AND GENDER-BASED CRIMES IN INDIA WITH REFERENCE TO DEEPFAKES AND ONLINE HARASSMENT

By *Dr Ritu Sharma*
Assistant Professor at BJR Institute of Law, Bundelkhand University, Jhansi

Abstract

The rapid evolution of Artificial Intelligence (AI) has significantly transformed digital interactions, but it has also ushered in new and insidious forms of gender-based violence. Among the most concerning developments is the emergence of *deepfakes*—AI-generated synthetic media—and algorithm-driven online harassment, which disproportionately target women and marginalized genders. This paper critically examines the intersection of AI and gender-based cybercrimes in India, focusing on the legal and social challenges posed by deepfakes and AI-enabled abuse. It investigates the limitations of the existing Indian legal framework, including the Information Technology Act, 2000, and the Indian Penal Code, 1860, which lack the definitional precision and procedural tools to tackle AI-specific offences. Through comparative legal analysis of jurisdictions such as the UK, South Korea, the US, and China, the study explores how progressive models address deepfake crimes through platform regulation, victim protection, and criminalisation of non-consensual synthetic media. The paper concludes with actionable recommendations for India's legal and policy framework, advocating for a rights-based, victim-centric, and technologically adaptive approach. This research underscores the urgent need for India to develop comprehensive legal tools that not only criminalise AI-facilitated gender violence but also promote digital justice and online safety for all.

Keywords
Artificial Intelligence, Deepfakes, Gender-Based Cybercrime, Online Harassment, Indian Cyber Law, Information Technology Act, Digital Violence, Non-consensual Imagery, Comparative Law, Victim Rights

1. Introduction

The advent of Artificial Intelligence (AI) has revolutionised digital ecosystems across sectors—ranging from healthcare and finance to governance and media. However, alongside its potential for socio-economic development, AI also presents unique ethical and legal challenges, particularly in the context of gender-based violence online. Nowhere is this more evident than in the proliferation of deepfake technologies and AI-enabled online harassment, which disproportionately affect women and marginalised gender identities. Deepfakes are synthetic media—images, audio, or video—generated using machine learning techniques such as Generative Adversarial Networks (GANs). These tools allow individuals to fabricate realistic-looking videos or images by superimposing someone's face or voice onto another's body or dialogue, often without consent.[1] When used maliciously, such content becomes a potent tool for non-consensual pornography, morphing, revenge porn, and character assassination, all of which constitute serious intrusions into an individual's privacy and bodily autonomy.[2] In the Indian context, the intersection of AI and gender-based violence has become increasingly prominent. According to the Cyber

[1] A Dey & SK Dey, *Leveraging AI in Prevention and Protection of Women Against Cybercrime in India: A Paradigm Shift of Criminal Law in the Making*, in Proceedings of the International Ethical Hacking Conference (Springer, 2024) 229–240, https://link.springer.com/chapter/10.1007/978-981-97-8457-8_20

[2] R de Silva de Alwis, *Gendering the New International Convention on Cybercrimes and New Norms on Artificial Intelligence and Emerging Technologies*, Wash. JL Tech. & Arts (2024), https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/washjolta20&section=7

Crime Reports of the National Crime Records Bureau (NCRB), incidents related to online sexual harassment and publication of obscene content have been rising, with women being the primary targets.[3] These crimes have evolved with technology: what began as online trolling and cyberstalking has morphed into AI-enabled impersonation and algorithmically curated sexual content, often distributed across social media without the victim's knowledge or consent.[4]

Despite these developments, India's current legal framework remains technologically outdated and structurally inadequate. The Information Technology Act, 2000, the country's primary legislation for cyber offences, does not specifically criminalise deepfake technology or AI-generated harms. While sections such as 66E, 67, and 67A address violation of privacy and publication of obscene material, they are often difficult to invoke when perpetrators remain anonymous or when the content is synthetic, yet indistinguishably realistic.[5] The Indian Penal Code (IPC) does provide certain remedies under Sections 354C (voyeurism), 499 (defamation), and 509 (outraging modesty of women), but these too were framed in a pre-AI era, lacking relevance in a digitally mediated society.[6]

Globally, several jurisdictions have begun to address AI-related gender-based crimes. For example, the UK's Online Safety Act, 2023, and South Korea's amendments to its Sexual Violence Crime Act specifically outlaw the creation and dissemination of sexual deepfakes.[7] India, however, is yet to legislate any deepfake-specific legal framework, making it crucial to re-evaluate how technological harms intersect with gender justice in the digital era.

This paper seeks to critically analyse the growing threat of AI-enabled gender-based crimes in India, with a specific focus on deepfakes and online harassment, while evaluating the gaps in the current legal infrastructure and offering comparative and reformative suggestions based on global practices.

2. Understanding Deepfakes and AI-Enabled Harassment

The digital revolution has led to a profound transformation in the way individuals interact, communicate, and access information. However, this technological advancement has also given rise to new forms of harm, particularly gendered harm, which exploit the anonymity, reach, and sophistication of AI-based tools. Among the most notorious innovations in this context are deepfakes — AI-generated synthetic media — and AI-facilitated online harassment, which are increasingly used to target, silence, and shame women in the digital space.

2.1 What Are Deepfakes?

The term "deepfake" is derived from "deep learning", a subset of machine learning, and "fake", indicating the synthetic nature of the media. Deepfakes are created using Generative Adversarial Networks

[3] National Crime Records Bureau (NCRB), *Crime in India Report 2023*, Ministry of Home Affairs, Government of India (2024), available at https://ncrb.gov.in

[4] S Yumkhaibam, *Digital Gender-Based Violence: Power, Inequality, and the Struggle for Online Safety in India*, Academia.edu (2025), https://www.academia.edu/download/124247485/Power_Inequality_and_Struggle_for_Online_Safety_Sushmita_.pdf

[5] Debasrita Choudhury, *Technology and Its Impact on Gender Disparity: An Analysis with Special Reference to Artificial Intelligence*, (ILI Dissertation, 2024), http://14.139.185.167:8080/jspui/bitstream/123456789/1486/1/LM0123005%20Debasrita%20Choudhury.pdf

[6] J Yadav & A Parihar, *Deepfakes: The Nexus of Technology and Crime*, SSRN Working Paper Series (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5296147

[7] KC Mythili & K Nagamani, *Safeguarding Women in Digital Spaces: Legal Responses to Cyber Harassment and Objectification on Social Media*, *Development Policy Review*, Wiley Online Library (2025), https://onlinelibrary.wiley.com/doi/abs/10.1111/dpr.70039

(GANs), wherein two neural networks — a generator and a discriminator — compete to produce media that is indistinguishable from authentic content.[8] This process enables the superimposition of a person's face, voice, or body onto another individual's video or audio, often without their consent. The weaponization of deepfakes has gained significant traction in the realm of gender-based violence. According to a study by Sensity AI, 96% of deepfake videos online were pornographic, and 99% of the subjects were women, usually without their knowledge or consent.[9] This form of non-consensual deepfake pornography not only violates privacy but also inflicts severe psychological and reputational damage, amounting to a digital form of sexual violence. Deepfakes are especially dangerous in patriarchal societies like India, where a woman's reputation is closely tied to family honour and social acceptance. In numerous reported cases, women have been subjected to "morphed pornography", wherein their faces are mapped onto explicit material and circulated through messaging platforms like WhatsApp and Telegram, resulting in public shaming, job loss, or even suicide.[10] The invisibility of the perpetrator, ease of dissemination, and difficulty in verifying synthetic content pose unique challenges to traditional legal frameworks. Victims often find little recourse, as law enforcement lacks the technological expertise to trace or remove such content effectively.[11]

2.2 Online Harassment Through AI

Artificial Intelligence extends beyond the realm of deepfakes to facilitate various other forms of online harassment, including but not limited to:

- AI-generated bots that mass-harass women on social media using misogynistic slurs and sexualized language.
- Impersonation algorithms that create fake profiles or manipulate voice recordings to impersonate victims.
- AI-facilitated doxxing, where personal information is scraped and disseminated with malicious intent.
- Synthetic blackmail, involving fabricated audio or video used to extort or coerce victims into silence.

In India, a particularly infamous case was the "Bulli Bai" and "Sulli Deals" incidents, where AI tools were allegedly used to scrape photos of Muslim women from social media and present them as auctionable "items" through mock online platforms.[12] While the police were able to track the perpetrators, the damage was already done, as the platforms were hosted anonymously and the content was shared across borders. AI also enables "algorithmic harassment", where platforms unintentionally amplify abusive content. Recommendation engines on platforms like YouTube and Instagram may push degrading content about women to wider audiences, effectively normalizing gendered hate.[13] The cyber infrastructure in India is ill-equipped to handle such nuanced AI

[8] T Nazakat & F Malik, *Empowering Justice through AI: Addressing Technology-Facilitated Gender-Based Violence*, *Journal of Law and Social Studies* (2025) 102–116, https://www.advancelrf.org/wp-content/uploads/2025/04/Vol-7-No.-1-3.pdf

[9] Sensity AI, *The State of Deepfakes: 2023 Report*, https://sensity.ai/reports/the-state-of-deepfakes-2023/

[10] Aman Gautam et al., *Mitigating Human Rights Violations Caused by Deepfake Technology*, *Library of Progress* (2024) https://www.researchgate.net/profile/Aman-Gautam-8/publication/384765955_Mitigating_Human_Rights_Violations_Caused_by_Deepfake_Technology

[11] D Mishra, *Deepfake Videos as a Form of Gender Violence*, in *Educating Women on Cyber-Feminism*, Springer (2025) 155–167, https://link.springer.com/chapter/10.1007/978-3-031-95619-5_13

[12] KC Mythili & K Nagamani, *Safeguarding Women in Digital Spaces: Legal Responses to Cyber Harassment*, *Development Policy Review* (2025) https://onlinelibrary.wiley.com/doi/abs/10.1111/dpr.70039

[13] Debasrita Choudhury, *Technology and Its Impact on Gender Disparity: An Analysis with Special Reference to Artificial Intelligence*, ILI Dissertation (2024) http://14.139.185.167:8080/jspui/bitstream/123456789/1486/1/LM0123005%20Debasrita%20Choudhury.pdf

threats. The Information Technology Act, 2000, while addressing issues such as publication of obscene material under Sections 67 and 67A, does not account for automated AI systems as perpetrators or AI-generated synthetic media. The lack of definitional clarity in Indian law around digital impersonation, algorithmic harassment, and synthetic content weakens the ability of victims to seek justice.[14]

The evidentiary challenges posed by AI-generated content make legal remedies difficult. Courts are yet to evolve standards on the admissibility, authenticity, and forensic analysis of synthetic content. This results in impunity for perpetrators and further marginalisation of victims in the digital space.[15]

3. Gendered Implications in the Indian Context

The emergence of artificial intelligence as a facilitator of digital crimes has magnified pre-existing gender disparities in India, a society already marred by deep-rooted patriarchal structures. AI-enabled threats such as deepfakes, image-based sexual abuse (IBSA), and algorithmic harassment have become powerful tools to silence, shame, and exclude women from public and digital spaces. Unlike random acts of cybercrime, AI-based gender crimes are systematically targeted and exhibit a strong gendered dimension — a reflection of technological patriarchy embedded in digital design, platform algorithms, and enforcement mechanisms. Studies reveal that women, particularly female journalists, activists, and influencers, are at higher risk of being deepfaked, stalked, or impersonated using AI tools.[16]

The social repercussions for women in India are disproportionately severe. Victims of deepfake pornography or online harassment often experience:

- Stigmatization and loss of reputation in conservative communities.
- Withdrawal from education or employment due to public shame.
- Mental health issues, including anxiety, depression, and suicidal ideation.[17]

In this climate, the role of law becomes not merely punitive but also protective and restorative. However, the Indian legal framework remains technologically inadequate in responding to the gendered implications of AI-based crimes.

3.1 Existing Legal Framework in India

India's legal response to technology-facilitated gender-based violence is largely reactive, fragmented, and rooted in a pre-AI understanding of crime. Although various laws address aspects of online abuse and obscenity, none explicitly criminalize AI-generated deepfakes, algorithmic impersonation, or synthetic media offences.

a) Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is India's principal cyber legislation. While it does not specifically address deepfakes or AI harms, the following provisions are invoked in related cases:

[14] Zubair A. Khan & Asma Rizvi, *Deepfakes: A Challenge for Women Security and Privacy*, *CMR Journal of Contemporary Legal Affairs* (2024) https://www.cmr.edu.in/.../Deepfakes-A-Challenge-for-Women-Security-and-Privacy.pdf

[15] R. de Silva de Alwis, *Gendering Cybercrime and New Norms on AI*, *Washington Journal of Law, Technology & Arts* (2025), https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/washjolta20&section=7

[16] Ibid

[17] S Yumkhaibam, *Digital Gender-Based Violence: Power, Inequality, and the Struggle for Online Safety in India*, Academia (2025), https://www.academia.edu/download/124247485/Power_Inequality_and_Struggle_for_Online_Safety_Sushmita_.pdf

- Section 66E: Punishes the violation of privacy by capturing, publishing, or transmitting images of a person's private parts without consent.[18]
- Section 67: Deals with the publication or transmission of obscene material in electronic form.
- Section 67A: Penalizes publishing or transmitting material containing sexually explicit acts.

These provisions are inadequate for AI-generated content, as they were framed with human actors and manual publication in mind. For instance, synthetic pornography created through GANs does not involve actual sexual acts, making it difficult to prosecute under Section 67A.[19] These sections do not account for the role of algorithms, platforms, or automated bots, which are central to the propagation of deepfakes.

b) Indian Penal Code, 1860

Several provisions of the Indian Penal Code (IPC) are applied in cases of online gender-based crimes:

- Section 354C (Voyeurism): Criminalizes capturing and sharing images of a woman without her consent.
- Section 499 & 500 (Defamation): Provide remedies for harm to reputation through false content.
- Section 509: Penalizes words, gestures or acts intended to insult the modesty of a woman.

Yet again, these laws are often inapplicable to AI-generated content, where the imagery may be synthetic and not actually captured from the victim. The requirement of actual bodily exposure or real-world filming often excludes deepfake-based violations from legal remedy.[20]

c) Absence of Deepfake-Specific Legislation

Despite the growing global consensus on regulating deepfakes — with countries like the UK, South Korea, and China passing targeted legislation — India currently lacks a comprehensive legal framework to address the menace. While the Personal Data Protection Bill, 2023 and Digital India Act (proposed) mention consent and data security, there is no explicit criminalisation of AI-based impersonation or synthetic pornography.[21]

This regulatory vacuum results in:

- Delayed FIR registrations, as police often don't recognise deepfakes as criminal.
- Judicial ambiguity, since courts lack precedents on admissibility of AI-generated evidence.
- Victim-blaming, as the burden of proof often shifts to women to demonstrate that the content is fake.

In the absence of effective redressal mechanisms, many victims resort to silence or social withdrawal, contributing to the digital exclusion of women and curtailment of their right to free expression.

4. Jurisprudential Challenges

Artificial Intelligence (AI), particularly in the context of deepfakes and gender-based cybercrimes, presents several jurisprudential dilemmas in India. These

[18] Information Technology Act, 2000, Section 66E, Ministry of Law and Justice, Government of India.
[19] KC Mythili & K Nagamani, *Safeguarding Women in Digital Spaces: Legal Responses to Cyber Harassment*, *Development Policy Review*, Wiley (2025), https://onlinelibrary.wiley.com/doi/abs/10.1111/dpr.70039
[20] Zubair A. Khan & Asma Rizvi, *Deepfakes: A Challenge for Women Security and Privacy*, *CMR Journal of Contemporary Legal Affairs* (2024), https://www.cmr.edu.in/school-of-legal-studies/journal/wp-content/uploads/2024/01/Deepfakes-A-Challenge-for-Women-Security-and-Privacy.pdf
[21] A Dey & SK Dey, *Leveraging AI in Prevention and Protection of Women Against Cybercrime in India: A Paradigm Shift of Criminal Law in the Making*, Springer (2024), https://link.springer.com/chapter/10.1007/978-981-97-8457-8_20.

challenges not only concern substantive law but also procedural hurdles, evidentiary complexities, and enforcement asymmetries.

One of the foremost concerns is attribution of liability. Deepfake technology relies on generative algorithms, which allow the anonymization of perpetrators and decentralization of content production. Courts often struggle with pinning accountability when the tool used is self-learning and the perpetrator hides behind VPNs or foreign servers. Traditional doctrines of mens rea (guilty mind) become blurry in the AI realm, especially when AI is used as an intermediary agent rather than a direct tool of offense[22].

Second, there is a lack of clarity in statutory interpretation. Indian cyber laws such as Section 66E and Section 67A of the Information Technology Act, 2000 (as amended) do address voyeurism and sexually explicit content, but deepfakes occupy a grey area. When a non-consensual deepfake does not involve actual nudity or pornographic elements but still harms dignity and reputation, it challenges current legal thresholds[23]. Further, evidentiary admissibility poses a significant hurdle. While Sections 65A and 65B of the Indian Evidence Act, 1872 allow digital evidence, courts are often ill-equipped to verify the authenticity of synthetic media. Establishing the "chain of custody" of manipulated digital content is complex, especially in a decentralized and ephemeral online environment[24]. Jurisdictional issues also plague prosecution. A deepfake created abroad but circulated in India may not fall neatly within Indian legal jurisdiction. The Budapest Convention on Cybercrime, which India has not ratified, could have provided a framework for international cooperation in such cases[25]. Moreover, the "chilling effect" of prosecution must be balanced with the right to free speech and expression under Article 19(1)(a) of the Indian Constitution. Courts have so far hesitated to define the limits of parody and satire in AI-generated content, especially when these overlap with political dissent or sexual expression[26]. A jurisprudential gap also exists in gender-sensitive interpretations of harm. AI-generated deepfakes disproportionately target women, particularly public figures and journalists. Yet, the courts have seldom articulated a doctrine of "gendered harm", despite calls for feminist jurisprudence to address technology-facilitated violence[27]. Lastly, sentencing frameworks have yet to catch up. Deepfakes, despite their potentially devastating impact, are rarely punished proportionately. This undercuts both deterrence and victim justice.

5. Victim-Centric Consequences

The proliferation of deepfakes and AI-enabled online harassment in India disproportionately targets women, inflicting severe psychological, social, and economic consequences. These impacts extend far beyond the digital domain, often disrupting the victim's real-world relationships, career prospects, and mental health stability.

Firstly, psychological trauma is one of the most immediate and profound effects experienced by victims of AI-generated sexual content, including deepfakes. Victims often suffer from post-traumatic

[22] Hall, M., Pester, A., & Atanasov, A. (2022). *AI Threats to Women's Rights: Implications and Legislations*. *Journal of Law and Emerging Technologies*. Available at JOLETS

[23] Choudhury, D. (2024). *Technology and its Impact on Gender Disparity: an Analysis with Special Reference to Artificial Intelligence*. Available at NLU Digital Repository

[24] Barman, S. (2025). *Cybercrime Against Women: How Cybercrime Targets Women's Privacy and Security*. *ResearchGate*. Link to full text

[25] Nazakat, T., & Malik, F.E. (2025). *Empowering Justice through AI: Addressing Technology-Facilitated Gender-Based Violence with Advanced Solutions*. *Journal of Law & Social Studies*. Download PDF

[26] Anjana, L. (2024). *Unveiling E-Shadows: Understanding Women's Cyber Victimisation*. *NUALS Law Journal*. Available on HeinOnline

[27] Halder, D., & Basu, S. (2025). *Digital dichotomies: Navigating non-consensual image-based harassment and legal challenges in India*. *Information & Communications Technology Law*.

stress disorder (PTSD), depression, anxiety, and in severe cases, suicidal ideation, especially when manipulated images are circulated widely without consent[28]. A report by Gaur and Jamal emphasizes that the unauthorized circulation of intimate AI-generated media leaves lasting psychological scars, particularly in a society like India where victim-blaming is rampant and privacy norms are fragile[29]. Secondly, the social stigma surrounding such crimes in Indian society exacerbates the isolation of victims. Many women are ostracized by family or community, fearing dishonour, regardless of the fact that the content was fabricated. As noted in *Psybersecurity: Human Factors of Cyber Defence*, the deeply entrenched patriarchal norms in Indian society often result in the revictimization of women through moral judgment rather than support[30]. This societal failure not only isolates the victim but also silences future reporting of similar offences. Additionally, AI-enabled harassment has a chilling effect on women's participation in public and professional spheres. Female journalists, influencers, and public figures have increasingly reported threats of deepfake attacks aimed at undermining their credibility or coercing silence[31]. This trend reinforces digital exclusion, where women retreat from online platforms for fear of targeted abuse.

From an economic standpoint, deepfake-related harassment often leads to loss of employment opportunities, particularly in sectors requiring public presence or digital branding. Employers may not differentiate between real and fake content, leading to withdrawal of job offers or reputational harm[32]. A critical dimension is the inadequacy of victim-support mechanisms. While India has laws against image-based abuse, there is no dedicated crisis response infrastructure to assist victims of AI-manipulated content. A study by Singh and Shanker (2024) critiques the lack of trained personnel in cyber cells, highlighting that most officers lack forensic capabilities to analyze and verify deepfakes[33]. Furthermore, there are no legal provisions for timely takedown, leaving victims exposed to prolonged harm.

6. Global Perspectives and Comparative Law

As the use of artificial intelligence in facilitating gender-based cybercrimes—particularly through deepfakes and AI-enabled harassment—grows, several countries have adopted progressive legal frameworks to address the challenge. These jurisdictions offer valuable insights for India, where legal provisions have lagged behind technological innovation.

United Kingdom (UK)

The UK has taken a proactive approach in regulating deepfakes, especially those involving non-consensual intimate imagery. The Online Safety Act 2023 introduces criminal liability for sharing deepfake pornography without consent, treating it similarly to

[28] Sharma, A., Agarwal, K., & Singh, T. (2024). *Exploring AI-Enabled Crime: An In-Depth Analysis of Pornographic Image Morphing*. In *Artificial Intelligence and Cyber Security* (Taylor & Francis).

[29] Gaur, V. & Jamal, N. (2024). *Human Rights and Artificial Intelligence: Addressing Emerging Threats to Humanity in Indian Context*. *International Journal of Social Science Research*, 2(4).

[30] Wood, A. (2024). *Dark Echoes: The Exploitative Potential of Generative AI in Online Harassment*. In *Psybersecurity: Human Factors of Cyber Defence*. Taylor & Francis

[31] Pashentsev, E., & Bazarkina, D. (2023). *Malicious Use of Artificial Intelligence: Risks to Psychological Security in BRICS Countries*. Springer.

[32] Singh, A. & Shanker, N. (2024). *Redefining Cybercrimes in Light of Artificial Intelligence: Emerging Threats and Challenges*. *International Journal of Innovations in Science, Engineering and Management*.

[33] Dey, A. & Dey, S.K. (2024). *Leveraging AI in Prevention and Protection of Women Against Cybercrime in India: A Paradigm Shift of Criminal Law in the Making*. Springer.

revenge porn.[34] The legislation empowers Ofcom to fine platforms that fail to remove harmful AI-generated content promptly. Additionally, the Law Commission's 2022 recommendations advocated for a new offence specifically targeting the creation and dissemination of deepfakes, irrespective of whether they involve nudity—acknowledging the emotional and reputational harm caused even in non-sexual contexts.[35]

United States (US)

In the U.S., there is no comprehensive federal legislation targeting deepfakes, but several states have enacted laws. California and Virginia have criminalized the use of deepfakes in pornography and political misinformation, especially during elections.[36] The U.S. approach is sectoral and fragmented, focusing more on freedom of speech considerations under the First Amendment. However, initiatives like the DEEPFAKES Accountability Act (proposed in Congress) seek to mandate disclosure of synthetic media and criminalize malicious creation of deepfakes, particularly those used to harass or defame individuals[37].

Courts in the U.S. have also relied on civil remedies, such as defamation, privacy torts, and the intentional infliction of emotional distress, to provide relief to victims of AI-generated abuse[38].

South Korea

South Korea stands as a pioneer in criminalizing deepfake content. The 2020 amendment to the Act on Special Cases Concerning the Punishment, etc., of Sexual Crimes makes the production, distribution, and possession of sexually explicit deepfakes punishable with imprisonment, even if consent was given for the original image.[39] Enforcement is relatively robust, aided by specialized cyber units and AI forensic tools developed by the Korean National Police Agency. South Korea's law is victim-centric and acknowledges the psychological damage suffered due to the synthetic nature of the harm.

China

China has adopted an authoritarian yet technologically advanced approach. Under the Provisions on the Administration of Deep Synthesis Internet Information Services (2023), all deepfake content must bear watermarks and disclaimers, and providers must ensure that AI content is non-deceptive and non-defamatory.[40] China treats deepfakes as a data governance issue under its Personal Information Protection Law (PIPL) and Cybersecurity Law, rather than as a purely criminal matter. Violations can lead to heavy fines and shutdowns of digital platforms.

Comparative Observations for India

Compared to these jurisdictions, India's approach remains reactive, non-specific, and procedurally opaque. The Information Technology Act, 2000 and Indian Penal Code offer only broad protections against

[34] UK Online Safety Act 2023. Available at: https://www.legislation.gov.uk/ukpga/2023/45/enacted

[35] Law Commission (2022). *Harmful Online Communications: The Criminal Law Proposals*, UK Gov. https://www.lawcom.gov.uk/project/harmful-online-communications/

[36] California Assembly Bill No. 602 (2021) and Virginia Code § 18.2-386.2. [U.S. State Legislature Portals].

[37] DEEPFAKES Accountability Act, H.R.3230, 116th Congress (2019). [U.S. Congress Records].

[38] Vijeyarasa, R. (2023). *Gendered Harms and the Regulation of Artificial Intelligence: A Comparative Assessment of Emerging Legislative Practice*. *Notre Dame Journal of Emerging Technologies*, 5. HeinOnline

[39] Ogunyemi, A. et al. (2025). *Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience*. *Future Internet*, 17(7), 309. MDPI

[40] Pashentsev, E. & Bazarkina, D. (2023). *Malicious Use of AI and Deepfake Regulation in BRICS Countries*. In: *Palgrave Handbook on AI Security*. Springer. [DOI: 10.1007/978-3-031-22552-9_20]

obscenity or defamation, with no provisions specifically aimed at synthetic content or deepfake technologies. While the Digital India Act (Draft, 2024) is expected to fill some gaps, it is yet to be enacted. Moreover, India lacks specialized cybercrime tribunals, AI forensic capabilities, and cross-jurisdictional enforcement tools, all of which are now emerging in more AI-aware legal systems.

A comparative synthesis reveals that countries with effective AI-regulation tend to:

- Define deepfakes and synthetic content in law.
- Criminalize non-consensual AI-generated imagery directly.
- Regulate platforms for timely removal and content flagging.
- Equip law enforcement with digital forensic tools.
- Provide victim-centric remedies, including compensation and psychological support.

India could benefit immensely from adopting a hybrid model, combining UK-style platform regulation, South Korea's penal clarity, and China's AI governance principles, while ensuring constitutional protection of rights like freedom of speech and privacy.

Conclusion and Recommendations

The integration of Artificial Intelligence (AI) into digital communication has opened new avenues for empowerment, but it has also intensified the scale, anonymity, and sophistication of gender-based cybercrimes, particularly in India. Deepfakes, algorithmic impersonation, and AI-enabled online harassment are not merely technological disruptions—they are manifestations of evolving patriarchal violence in a digitized society. Existing Indian legal instruments like the Information Technology Act, 2000, and the Indian Penal Code, 1860, remain ill-equipped to address the synthetic and cross-jurisdictional nature of AI-generated abuse, leaving victims vulnerable, silenced, and often without remedy. In comparison, jurisdictions such as South Korea, the UK, and China have begun to reshape legal architectures to explicitly criminalize and regulate deepfake technologies, offering India valuable legislative and procedural models.

To confront this emerging digital threat, India must adopt a multi-pronged, victim-centric, and technologically responsive legal framework. First, a clear statutory definition of "deepfake" and "AI-generated harmful content" must be introduced through amendments to the IT Act or the proposed Digital India Act. Second, India should criminalize non-consensual AI-generated intimate imagery, irrespective of whether real nudity or sexual activity is depicted, drawing from UK and South Korean approaches. Third, dedicated cybercrime cells must be strengthened with forensic AI capabilities, backed by judicial training on synthetic evidence and digital rights. Fourth, platforms must be obligated—under a revised intermediary liability regime—to deploy watermarking, detection, and takedown mechanisms for deepfake content, ensuring timely redressal. Finally, the response to AI-enabled gender violence must be intersectional, with the government investing in digital literacy, mental health support, and financial compensation schemes for affected women and marginalized communities.

The future of online safety, particularly for women and gender minorities, will be defined by the laws we shape today. A responsive, anticipatory, and rights-based regulatory ecosystem is no longer optional—it is essential to ensure technological justice in the age of AI.

References

1. A. Dey and S.K. Dey, *Leveraging AI in Prevention and Protection of Women Against Cybercrime in India: A Paradigm Shift of Criminal Law in the Making*, in *International Ethical Hacking Conference* (Springer, 2024), available at: https://link.springer.com/chapter/10.1007/978-981-97-8457-8_20.
2. R. de Silva de Alwis, *Gendering the New International Convention on Cybercrimes and New Norms on*

Artificial Intelligence and Emerging Technologies, *Washington Journal of Law, Technology & Arts*, 20 (2025), available at: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/washjolta20&section=7.

3. National Crime Records Bureau (NCRB), *Crime in India Report 2023*, Ministry of Home Affairs, Government of India, available at: https://ncrb.gov.in.
4. S. Yumkhaibam, *Digital Gender-Based Violence: Power, Inequality, and the Struggle for Online Safety in India*, Academia.edu (2025), available at: https://www.academia.edu/download/124247485/Power_Inequality_and_Struggle_for_Online_Safety_Sushmita_.pdf.
5. Debasrita Choudhury, *Technology and Its Impact on Gender Disparity: An Analysis with Special Reference to Artificial Intelligence* (ILI Dissertation, 2024), available at: http://14.139.185.167:8080/jspui/bitstream/123456789/1486/1/LM0123005%20Debasrita%20Choudhury.pdf.
6. Zubair A. Khan and Asma Rizvi, *Deepfakes: A Challenge for Women Security and Privacy*, *CMR Journal of Contemporary Legal Affairs* (2024), available at: https://www.cmr.edu.in/school-of-legal-studies/journal/wp-content/uploads/2024/01/Deepfakes-A-Challenge-for-Women-Security-and-Privacy.pdf.
7. T. Nazakat and F. Malik, *Empowering Justice through AI: Addressing Technology-Facilitated Gender-Based Violence with Advanced Solutions*, *Journal of Law & Social Studies* (2025), available at: https://www.advancelrf.org/wp-content/uploads/2025/04/Vol-7-No.-1-3.pdf.
8. Aman Gautam et al., *Mitigating Human Rights Violations Caused by Deepfake Technology*, ResearchGate (2024), available at: https://www.researchgate.net/publication/384765955.
9. Sharma, A., Agarwal, K., & Singh, T., *Exploring AI-Enabled Crime: An In-Depth Analysis of Pornographic Image Morphing*, in *Artificial Intelligence and Cyber Security* (Taylor & Francis, 2024), available at: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003518587-15.
10. Gaur, V. and Jamal, N., *Human Rights and Artificial Intelligence: Addressing Emerging Threats to Humanity in Indian Context*, *International Journal of Social Science Research*, Vol. 2, Issue 4 (2024), available at: https://www.ijssr.com/wp-content/uploads/journal/published_paper/volume-2/issue-4/IJSSR30536.pdf.
11. Wood, A., *Dark Echoes: The Exploitative Potential of Generative AI in Online Harassment*, in *Psybersecurity: Human Factors of Cyber Defence* (Taylor & Francis, 2024), available at: https://www.taylorfrancis.com/chapters/edit/10.1201/9781032664859-5.
12. Singh, A. and Shanker, N., *Redefining Cybercrimes in Light of Artificial Intelligence: Emerging Threats and Challenges*, *International Journal of Innovations in Science, Engineering and Management*, (2024), available at: https://ijisem.com/journal/index.php/ijisem/article/download/168/159.
13. UK Online Safety Act, 2023, available at: https://www.legislation.gov.uk/ukpga/2023/45/enacted.
14. Law Commission of England and Wales, *Harmful Online Communications: The Criminal Law Proposals* (2022), available at: https://www.lawcom.gov.uk/project/harmful-online-communications/.
15. California Assembly Bill No. 602 (2021) and Virginia Code § 18.2-386.2, accessible via respective U.S. State Legislature websites.
16. DEEPFAKES Accountability Act, H.R.3230, 116th Congress (2019), available at: https://www.congress.gov/bill/116th-congress/house-bill/3230.
17. Vijeyarasa, R., *Gendered Harms and the Regulation of Artificial Intelligence: A Comparative Assessment of Emerging Legislative Practice*, *Notre Dame Journal of Emerging Technologies*, Vol. 5 (2023), available at: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ndjet5&section=6.
18. Ogunyemi, A. et al., *Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience*, *Future Internet*,

17(7), 309 (2025), available at: https://www.mdpi.com/1999-5903/17/7/309.

19. Pashentsev, E. and Bazarkina, D., *Malicious Use of AI and Deepfake Regulation in BRICS Countries*, in *Palgrave Handbook on AI Security* (Springer, 2023), available at: https://doi.org/10.1007/978-3-031-22552-9_20.

*****