
WEAPONISED INTELLIGENCE - FROM DEEPPAKES TO SMART GLASSES: AI-ENABLED GENDER VIOLENCE AND THE CRISIS OF LEGAL PROTECTION FOR WOMEN IN INDIA

Dimple A. Parmar, Marwadi University

ABSTRACT

Artificial Intelligence was developed by human intelligence to make life simple and efficient, but today it is also being weaponised against women. This paper explains three weapons of AI-enabled gender violence: deepfakes, voice cloning and sextortion, and smart glasses such as the Ray-Ban Meta glasses. These tools are cheap, easy to use and anonymous, and they can harm a woman without her knowledge and without anyone touching her. The paper then examines whether Indian law protects women from this harm. It finds that although Articles 14, 15 and 21 of the Constitution promise equality, dignity and privacy, the IT Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023 and the IT Amendment Rules, 2026 are fragmented, focus on obscenity rather than consent, and regulate platforms rather than punish perpetrators. The paper calls these problems the *Authenticity Paradox* and *remedial fragmentation*. It compares the laws of the United Kingdom, the European Union, the United States and Australia, and suggests a way forward for India: a consent-based offence, regulation of AI tools and smart glasses, and a single authority where victims can seek help.

Keywords: Deepfakes, Non-Consensual Intimate Imagery, Voice Cloning, Sextortion, Smart Glasses, Consent, Right to Privacy.

Introduction

Earlier, a woman's dignity was violated online when her real private photograph or video was leaked. Today, AI has changed this completely. A woman does not need to have ever taken an intimate photograph for a fake intimate image of her to exist. One ordinary photograph from her Instagram profile, a few seconds of her voice, or a few moments in which a stranger's glasses record her on a train are enough. In India, cybercrime cases rose from 65,893 in 2022 to 86,420 in 2023,¹ and in January 2026 an AI tool on one of the world's largest social media platforms created sexualised images of real women on demand until governments, including India's, intervened.²

India's law has not kept pace with this change. The Constitution guarantees equality, dignity and privacy to every woman, but the statutes that should give effect to these guarantees were made for real photographs, physical acts and public morality. This paper argues that this gap is a crisis of legal protection for women. Chapter 1 explains how deepfakes, voice cloning and sextortion, and smart glasses are used against women, and the nature of the harm they cause. Chapter 2 examines the Constitution, the main statutes and the response of the courts. Chapter 3 compares the laws of the United Kingdom, the European Union, the United States and Australia. Chapter 4 rethinks the law and suggests a way forward, followed by the conclusion

1. Weaponised Intelligence: Deepfakes to Smart Glasses, AI-Enabled Gender Violence

Until AI came into existence, intelligence was a virtue of humankind alone. Humans used their intelligence, innovation and creativity to develop AI, so that it could simplify complex tasks, assist people and maximise output in all aspects of life. The development of AI is a great achievement of humankind. It is still at an early stage, and in the future it will become an inevitable part of human life, from birth to death.

However, like any other technological development in history, AI has two sides of a coin. On one side, it makes life better and simpler and increases efficiency. On the other side, its aim

¹ Nat'l Crime Records Bureau, Ministry of Home Affs., *Crime in India 2023* (2025); see also *NCRB 2023 Report: Rise in Crimes Against Women, Cybercrime, Farmer Suicides*, Nat'l Herald (Sept. 2025), <https://www.nationalheraldindia.com/national/ncrb-2023-report-rise-in-crimes-against-women-cybercrime-farmer-suicides>.

² Aleesha Sam, *Social Media Platform X 'Admits' Mistake over Grok Obscenity; 3,500 Posts Blocked, 600 Accounts Deleted After Govt Notice*, Free Press J. (Jan. 11, 2026), <https://www.freepressjournal.in/amp/india/social-media-platform-x-admits-mistake-over-grok-obscenity-3500-posts-blocked-600-accounts-deleted-after-govt-notice>.

and object have been misused: it has been weaponised to destroy the dignity and privacy of women and children beyond repair. It has become a tool for sexual abuse, harassment, stalking, intimidation and damaging reputation; it amplifies gender bias and gender inequality; and it creates psychological, social and political stigma against women. In this way, a tool developed by humans to imitate human intelligence has become a faceless weapon and a nightmare for half of the world's population: women. The vulnerability of women is not new, as women have been persecuted for thousands of years on the basis of gender and stereotypes. What is new is that AI amplifies this harassment, because AI tools are easily accessible, affordable, everywhere and anonymous in today's world of the internet.³

This chapter explains three weapons of AI-enabled gender violence, a form of Technology-Facilitated Violence Against Women: (i) deepfakes, (ii) voice cloning and sextortion, and (iii) smart glasses such as the Ray-Ban Meta glasses, along with the technology through which each of them harms women.

1.1 Deepfakes

A woman works at a reputed multinational company as a product supervisor. Along with her work, she actively participates in women-related issues and has a good social media presence. One day she shares her opinion on feminism, which other people find aggressive and liberal. Merely to express ordinary disagreement with her, one person takes her photo from her Instagram profile, creates a totally fake nude photo of her with a generative AI tool that creates realistic fake photos, and spreads it online. This dissemination damages her reputation, causes her psychological stress and results in her withdrawal from public life and from social media. These fake photos are known as deepfakes: a generative AI tool weaponised to humiliate women and to violate their dignity and privacy.

From its name, the word “deepfake” can be understood in two parts: “deep” refers to deep learning, and “fake” means forged, not real or true.⁴ A deepfake is synthetic media -an image, audio or video -created or changed by artificial intelligence so that it looks authentic or real. Non-Consensual Intimate Imagery (NCII) means the creation, capturing, publication or

³ See UN Women, *How AI Is Exacerbating Technology-Facilitated Violence Against Women and Girls* (2026), <https://www.unwomen.org/sites/default/files/2026-01/how-ai-is-exacerbating-technology-facilitated-violence-against-women-and-girls-en.pdf>.

⁴ U.S. Dep't of Homeland Sec., Sci. & Tech. Directorate, *S&T Digital Forgeries Report: Impacts of Generative Artificial Intelligence (Fiscal Year 2024 Report to Congress)* 14 (Jan. 17, 2025).

distribution of intimate images or videos without the consent of the person depicted.⁵ Deepfakes make NCII far more dangerous because, unlike traditional NCII, an AI-generated deepfake does not need an original intimate image of the victim; it can be made from an ordinary professional photograph. Deepfakes use deep learning methods such as GANs (Generative Adversarial Networks), which work by pitting two AI systems against each other: a Generator that creates fake images and a Discriminator that tries to detect them.⁶ They compete until the Generator becomes so good that the Discriminator -and eventually a human -cannot tell the difference.

The term originated in 2017 with a Reddit user who uploaded pornographic videos in which the faces of real women were swapped onto other people's bodies.⁷ This strongly suggests that the abuse of women is not a side effect of deepfakes; their very origin is attached to the abuse and harassment of women. This violence is an accelerated version of traditional, pre-AI digital violence. Before the advent of AI, women's modesty was also violated on digital media, but morphing an image required some skill and a morphed image was easily detected. After the advent of AI, the absence of any need for skill, the easy accessibility and availability of deepfake tools, growing social media use and an easy, unregulated process of dissemination have made women prey to this evil and inhuman practice of abuse. In 2023, the number of deepfake videos online was 95,820, an increase of 550 per cent since 2019; 98 per cent of them were pornographic, and 99 per cent of the people targeted in deepfake pornography were women.⁸ Globally, 38 per cent of women have personally experienced online violence, and 85 per cent have seen it happen to other women.⁹ The data show how technology-facilitated violence is different from traditional violence because of its scale, speed, ease of communication, anonymity, impunity, automation, affordability and undetectability.¹⁰

The clearest example of weaponised intelligence is the sexualised deepfake. In December 2025,

⁵ See Clare McGlynn & Erika Rackley, *Image-Based Sexual Abuse*, 37 Oxford J. Legal Stud. 534 (2017); *Mrs. X v. Union of India*, 2023 SCC OnLine Del 2361 (India).

⁶ Ian J. Goodfellow et al., *Generative Adversarial Networks* (2014), <https://arxiv.org/abs/1406.2661>; DHS, *Digital Forgeries Report*, *supra* note 4, at 20.

⁷ Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace, Sept. 2019).

⁸ Security Hero, *2023 State of Deepfakes: Realities, Threats, and Impact* (2023), <https://www.securityhero.io/state-of-deepfakes/>.

⁹ UN Women, *FAQs: AI-Powered Online Abuse: How AI Is Amplifying Violence Against Women and What Can Stop It* (Nov. 2025), <https://www.unwomen.org/en/articles/faqs/ai-powered-online-abuse-how-ai-is-amplifying-violence-against-women-and-what-can-stop-it>.

¹⁰ UN Women, *How AI Is Exacerbating TF VAWG*, *supra* note 3.

Grok, the AI tool of xAI that works both on its own and inside the social media platform X, allowed users to edit photos of real people with a simple text prompt. Within days, the feature was being used to create sexually explicit images, mainly of women and children, without their consent, and thousands of such images spread rapidly.¹¹ MeitY wrote to X on 2 January 2026, asking it to remove the content and to review Grok's safeguards, and in response X blocked about 3,500 posts and deleted more than 600 accounts in India.¹² The UK regulator Ofcom began an investigation into how Grok was being used to create "undressed images" of people,¹³ and Indonesia temporarily banned access to Grok.¹⁴ These incidents matter for two reasons when we talk about weaponised intelligence. First, how was a global social media platform able to produce sexualised content even though it had safeguards and a regulatory framework of its own? Second, after the incident, Grok limited its image generation feature to paid subscribers,¹⁵ making the creation of these images a "premium service".

Deepfakes are not limited to images; audio and video are also examples of technology-facilitated violence. As input, the technology needs only a few seconds of audio or video of a real person; through deep learning, it then creates the exact voice texture, accent, expression, mannerisms and behaviour of that person in fake audio and video. A McAfee survey found that three seconds of audio can be enough to clone a voice, and that 47 per cent of Indian respondents had either been victims of an AI voice scam or knew someone who had been.¹⁶ The US Department of Homeland Security confirmed in 2025 that "novel methods based on deep learning can produce speech that is indistinguishable from real speech."¹⁷ This capacity for voice replication is the foundation of the next category of AI-enabled violence examined in this chapter. In this way, a woman's identity, dignity, privacy and freedom of expression are violated without her consent, at a global scale, by a crime that is faceless, boundaryless and,

¹¹ *Musk's Grok Blocked by Indonesia, Malaysia over Sexualized Images in World First*, CNN (Jan. 12, 2026), <https://www.cnn.com/2026/01/12/business/indonesia-malaysia-grok-elon-musk-intl-hnk>.

¹² Sam, *supra* note 2.

¹³ *Grok Blocked in Indonesia and Malaysia as UK Launches Probe over Sexualised Images*, ABC News (Austl.) (Jan. 12, 2026), <https://www.abc.net.au/news/2026-01-12/grok-ai-blocked-in-indonesia-malaysia-over-explicit-images/106222336>.

¹⁴ *Indonesia Temporarily Blocks Access to Grok over Sexualised Images*, Reuters (Jan. 10, 2026), *reprinted in* ThePrint, <https://theprint.in/world/indonesia-temporarily-blocks-access-to-grok-over-sexualised-images/2823680/>.

¹⁵ *Id.*

¹⁶ McAfee, *Beware the Artificial Impostor: A McAfee Cybersecurity Artificial Intelligence Report* (May 2023); *see also Be Wary of AI-Assisted Crimes Using Cloned Voices and Faces*, Tribune (India) (Dec. 2023), <https://www.tribuneindia.com/news/comment/be-wary-of-ai-assisted-crimes-using-cloned-voices-and-faces-574842>.

¹⁷ DHS, *Digital Forgeries Report*, *supra* note 4, at 31.

under India's current legal framework, punishmentless.

1.2 Voice Cloning and Sextortion

As discussed above, voice cloning is a form of deepfake in which a person's voice is exactly replicated without his, her or their consent, and it is indistinguishable from the real voice. This leads to another crime called impersonation, where one person presents himself as another, steals that person's identity without consent and tries to extort money or influence the decisions of the general public. Women politicians and celebrities are the prime victims of this technology-facilitated violence because of their popularity and the easy availability of their photos, audio and videos, which can easily be turned into pornographic content to extort money. However, in India this is not limited to women politicians or celebrities; middle-class women have also become prey to this digital crime.

Two incidents occurred in Hyderabad. A 72-year-old homemaker lost Rs. 1.97 lakh after hearing what sounded like her sister-in-law's voice asking for money,¹⁸ and a 59-year-old woman lost about Rs. 1.4 lakh to a voice that sounded exactly like her nephew in Canada.¹⁹ These cases may look like ordinary financial fraud, but they show a pattern in which older women, and women who manage household relationships, are targeted through their emotional ties to family. It is high time for India to work towards regulating these crimes and punishing wrongdoers. This is only the beginning, and if these crimes are not regulated, Indian society will face new kinds of crime in the near future.

Sextortion is a serious crime, and AI facilitates it to a great extent by creating realistic fake videos of women in compromising positions, or clearly pornographic videos, which, when spread, cause great damage to a woman's reputation, and she is discriminated against and humiliated in every sphere of life. The National Commission for Women has therefore asked the Central Government to amend the law to clearly define and criminalise "deepfake abuse".²⁰ To stop the content from spreading, women have to pay huge amounts of money, which results

¹⁸ *Hyderabad Woman Falls Victim to AI Voice Scam, Loses Rs 1.97 Lakh*, Hans India (Mar. 2025), <https://www.thehansindia.com/telangana/hyderabad-woman-falls-victim-to-ai-voice-scam-loses-rs-197-lakh-954968>.

¹⁹ *A Woman from Hyderabad Loses 1.4 Lakh Rupees in an AI Scam*, IndiaAI (2023), <https://indiaai.gov.in/news/a-woman-from-hyderabad-loses-1-4-lakh-rupees-in-an-ai-scam>.

²⁰ *IT Act Toothless Against Deepfakes? NCW Seeks Review of Laggard Laws as Women Face More AI-Driven Abuse*, ThePrint (Nov. 2025), <https://theprint.in/india/it-act-toothless-against-deepfakes-ncw-seeks-review-of-laggard-laws-as-women-face-more-ai-driven-abuse/2786139/>.

in economic deprivation and leads to impoverishment. The effect of these crimes is not limited to the online world; it affects the day-to-day activities of women and makes them withdraw from every sphere of public life, which directly affects the political, economic, social and cultural representation of women. Women tend to take on a traditional role and limit themselves even when they have done nothing wrong. Not only are her consent, dignity, freedom and rights violated, but she also lives the life of a victim who never gets justice in the existing legal framework.

1.3 Smart Glasses (Ray-Ban Meta Smart Glasses)

Imagine a woman travelling in a metro in Mumbai. She is sitting casually in her seat and minding her own business when a stranger wearing glasses stands in front of her. Two days later, she finds that her video is circulating on Instagram. People are rating her appearance and making sexist comments, her DMs are flooded with messages, people are calling her, and she has become the centre of gossip at her workplace. Her privacy, identity and dignity have been violated by a stranger, because she did not know that her every expression and her body language were being recorded by glasses that looked ordinary but were actually Ray-Ban Meta smart glasses. According to the eyewear maker EssilorLuxottica, two million pairs were sold between October 2023 and February 2025.²¹

Unlike smartphones, smart glasses do not announce themselves. They rest on the face, blend naturally into a conversation and record everything without any notice to, or prior consent of, bystanders. Meta says that the glasses have a small LED that lights up while recording. However, a BBC investigation showed several videos in which the light can be covered or switched off, so that women are unaware of the recording.²² One woman, Dilara, aged 21, was approached during her lunch break in London. The video of her reached 1.3 million views and showed her phone number, after which she received a flood of calls and messages.²³ The devices have been nicknamed “pervert glasses”, and some places in the United Kingdom,

²¹ *Shares of Ray-Ban Maker EssilorLuxottica Jump 6% on Reported Meta Stake in AI Push*, CNBC (July 9, 2025), <https://www.cnbc.com/2025/07/09/shares-of-ray-ban-maker-essilorluxottica-jump-on-reported-meta-stake.html>.

²² *Women Filmed Secretly for Social Media Content – and Then Harassed Online*, Herald Times (Jan. 25, 2026), <https://www.heraldtimes.org/2026/01/25/women-filmed-secretly-for-social-media-content-and-then-harassed-online/> (reporting a BBC News investigation); see also *Smart Glasses and Privacy: Wearable Surveillance and Disclosure Issues*, Nat’l L. Rev. (Apr. 2026).

²³ *Id.*

including a pub chain, theatres and courts, have banned or restricted them.²⁴ These devices violate women's privacy not only in the private sphere but equally in the public sphere. The videos are recorded in public places, but what is taken is private information. This creates a new concept of "relational privacy", which means that its effect is not limited to the buyer of the product but extends to everyone around him.²⁵

The danger becomes clearer from an experiment by two Harvard University students, AnhPhu Nguyen and Caine Ardayfio, in 2024. In their project, called I-XRAY, they connected Ray-Ban Meta glasses to a program that detected faces in the video. Each face was searched on PimEyes, a public face-search website, and an AI tool then collected the person's name, address, phone number and even relatives' details within seconds.²⁶ The students said that they identified dozens of people, including Harvard students, without those people ever knowing.²⁷ Their aim was only to show the risk, but the experiment proves that these glasses are not just a camera. With freely available AI tools, a stranger who looks at a woman on a train can know her name and where she lives within a minute.

A lawsuit filed in the United States in March 2026, *Bartone v. Meta Platforms, Inc.*, relies on reports by two Swedish newspapers that workers at a Kenya-based subcontractor were reviewing clips captured by the glasses as part of an AI training process, and that these clips included nudity and other private moments inside homes.²⁸ In one incident described in the complaint, a man left his glasses on a bedside table, and his partner changed her clothes in front of them without knowing that they were recording.²⁹ The court has not yet decided whether these allegations are true, but they show that the harm from a wearable camera can reach the

²⁴ *Meta Ray-Bans Banned in UK Pubs and Theatres and the Smart Glasses Era Could Be Doomed*, Stuff (Aug. 2026), <https://www.stuff.tv/news/meta-ray-bans-banned-in-uk-pubs-and-theatres-and-the-smart-glasses-era-could-be-doomed/>; *England and Wales Ban Meta Glasses from Courtrooms*, Engadget (Aug. 2026), <https://www.engadget.com/2234606/england-and-wales-ban-meta-glasses-from-courtrooms/>.

²⁵ *See Smart Glasses and Privacy: Wearable Surveillance and Disclosure Issues*, Nat'l L. Rev. (Apr. 2026), <https://natlawreview.com/article/smart-glasses-and-privacy-wearable-surveillance-and-disclosure-issues>.

²⁶ John Koetsier, *Meta's Ray-Ban Smart Glasses Used to Instantly Dox Strangers in Public, Thanks to AI and Facial Recognition*, Forbes (Oct. 3, 2024), <https://www.forbes.com/sites/johnkoetsier/2024/10/03/metass-ray-ban-smart-glasses-used-to-instantly-dox-strangers-in-public-thanks-to-ai-and-facial-recognition/>; *Harvard Students Used Meta's Smart Glasses and AI to Get Private Info from People's Photos*, Bos. Globe (Oct. 4, 2024), <https://www.bostonglobe.com/2024/10/04/business/harvard-students-ai-meta-glasses/>.

²⁷ Koetsier, *supra* note 26.

²⁸ Class Action Complaint, *Bartone v. Meta Platforms, Inc.*, No. 3:26-cv-01897 (N.D. Cal. filed Mar. 2026); *Meta Sued over AI Smart Glasses' Privacy Concerns, After Workers Reviewed Nudity, Sex, and Other Footage*, TechCrunch (Mar. 5, 2026), <https://techcrunch.com/2026/03/05/meta-sued-over-ai-smartglasses-privacy-concerns-after-workers-reviewed-nudity-sex-and-other-footage/>.

²⁹ *Designed for Privacy? The Bartone v. Meta Litigation over AI Smart Glasses*, MediaLaws (July 2026), <https://www.medialaws.eu/designed-for-privacy-the-bartone-v-meta-litigation-over-ai-smart-glasses/>.

most private spaces of a woman's life.

1.4 The Nature of Harm

The three weapons explained above use different technologies, but the harm they cause to women is similar. First, it is sexual violence even though no one touches the woman. A fake sexual image shows her real face in a sexual act that she never did, and scholars treat this kind of image-based abuse as a form of sexual violence.³⁰ Second, the harm is psychological and continuous. Victims describe it as a “social rupture” that divides their life into before and after, and they live in constant fear that the image will appear again.³¹ As the Delhi High Court has said, the internet never forgets.³²

Third, the harm is social and economic. In Indian society, a woman whose fake image is circulated may face blame from her own family and community, problems in marriage and gossip at her workplace, and she may have to pay money to stop the content or lose her job. Fourth, the harm silences women. The United Nations has noted that deepfakes are used to harass and blackmail women and to drive them out of the online public sphere.³³ Fifth, the harm often happens without the woman's knowledge, so she cannot give or refuse consent. Finally, when fake images become so real, even genuine evidence of abuse can be called “fake”, which makes it harder for women to prove what happened to them.³⁴ All these harms strike at the dignity, privacy, autonomy and equality of women. They are not just crimes against public morality; they are violations of fundamental rights.

2. Legal Statutes Dealing With AI-enabled Abuse In India

Law is a system of rules, regulations, rights and obligations; individuals face punishment if they break these rules and harm the rights of others. This is the fundamental and philosophical concept of law. When a system or law does not protect the rights and dignity of an individual, it creates a draconian or inhuman environment; it affects not only the individual, but society

³⁰ McGlynn & Rackley, *supra* note 5.

³¹ Clare McGlynn et al., ‘It’s Torture for the Soul’: *The Harms of Image-Based Sexual Abuse*, 30 Soc. & Legal Stud. 541 (2021).

³² *X v. Union of India*, 2021 SCC OnLine Del 1788 (India).

³³ Office of the U.N. High Comm’r for Hum. Rts., *Call for Inputs: 2026 Thematic Report on Gender Equality in the Digital Space and Age* (2025), <https://www.ohchr.org/en/calls-for-input/2025/call-inputs-2026-thematic-report-gender-equality-digital-space-and-age>.

³⁴ DHS, *Digital Forgeries Report*, *supra* note 4, at 6.

also pays the price. This is exactly what is happening in India, where there is little or only fragmented law to punish or prevent AI-enabled violence against women. The constitutional mandates, the IT Act, the BNS, the Digital Personal Data Protection Act, 2023 and the IT Amendment Rules, 2026 are all fragmented laws, and they do not provide a clear solution to the growing problems of Technology-Facilitated Violence Against Women.

2.1 Constitutional Aspiration

2.1.1 Right to Dignity and Privacy

The Constitution of India takes pride in being progressive and liberal, and a protector and provider of human rights. Article 21 guarantees that no person shall be deprived of his life and personal liberty except according to procedure established by law.³⁵ The Supreme Court has long held that the right to life means more than mere animal existence and includes the right to live with human dignity.³⁶ In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge bench unanimously held that the right to privacy is a part of Article 21 and is protected under Part III.³⁷ The Court recognised and protected three core aspects of privacy: (1) bodily integrity, (2) informational privacy and (3) decisional autonomy.³⁸

Deepfakes or non-consensual intimate imagery violate these three aspects of privacy at their core. The creation and dissemination of fake images, audio or video infringe the bodily integrity of a woman, because they show a fake body with her real face and go against how she wants to portray herself in public. A sexualised deepfake disseminates a woman's face, words, expressions and personal details without her consent, and thereby infringes her informational privacy. It also takes away a woman's decisional autonomy over how she wants to engage in public. NCII is therefore not only a crime; it violates the fundamental rights to privacy and dignity.

2.1.2 Right to Equality and Special Protection for Women

Article 14 guarantees equality before the law and equal protection of the laws. Article 15(1) forbids discrimination on grounds of sex, and Article 15(3) allows the State to make special

³⁵ India Const. art. 21.

³⁶ *Francis Coralie Mullin v. Adm'r, Union Territory of Delhi*, (1981) 1 SCC 608 (India).

³⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

³⁸ *Id.* (Chandrachud, J.).

provisions for women. Article 51A(e) also places a duty on every citizen to renounce practices that are derogatory to the dignity of women.³⁹

The philosophy of Article 14 is that likes should be treated alike and unlikes should not be treated alike; in the same way, Article 15(3) empowers the State to make special provisions for women. In today's digital era, it seems on the surface that everyone is getting an equal footing, opportunity and treatment, but in reality AI itself is biased, and its algorithms run on gender bias, which is proved by the prevalence of technology-facilitated violence against women and children. A core reason for this bias is that the AI industry is dominated by men and lacks a female perspective at its core (only about 30 per cent of the world's AI professionals are women).⁴⁰ Hence, women need special protection to protect their dignity and freedom. The Supreme Court's reasoning in *Joseph Shine v. Union of India*, which struck down the offence of adultery because it treated a woman as her husband's property and denied her dignity and sexual autonomy, shows that the Court now reads equality and dignity together.⁴¹ In *Vishaka v. State of Rajasthan*, the Court went further and framed binding guidelines on workplace sexual harassment, drawing on international law, when Parliament had not yet acted.⁴² *Vishaka* is an important reminder that courts can act creatively when the law lags behind a gendered harm.

2.1.3 Constitutional Limitation

Fundamental rights are mainly enforceable against the State, but most perpetrators of AI-enabled abuse are private individuals or private companies. Therefore, the Constitution sets values and principles, but it cannot provide a quick and effective remedy to a woman whose dignity and freedom have been violated by AI-enabled abuse. For that, Parliament needs to create clear statutory and procedural rights.

2.2 Indian Statutes

2.2.1 The Information Technology Act, 2000

The IT Act, 2000 is India's primary cyber law. Several of its provisions can apply to AI-enabled

³⁹ India Const. arts. 14, 15, 51A(e).

⁴⁰ World Econ. F., *Global Gender Gap Report 2023* (June 2023).

⁴¹ *Joseph Shine v. Union of India*, (2019) 3 SCC 39 (India).

⁴² *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241 (India).

abuse, although it neither defines AI-enabled abuse nor provides a comprehensive and clear remedy. This creates a condition of *remedial fragmentation*: victims are compelled to navigate multiple provisions across multiple statutes to obtain a just remedy, which only increases their suffering.

Section 66C punishes whoever fraudulently or dishonestly makes use of any person's electronic signature, password or any other unique identification feature, with imprisonment of up to three years.⁴³ However, what constitutes a "unique identification feature" has not been settled by judicial interpretation. Whether a person's face or voice falls within its ambit remains an open question -one that must be urgently answered, because both are now routinely used for biometric recognition in everyday digital life.

Section 66D punishes cheating by personation through a computer resource.⁴⁴ Voice cloning incidents, in which a woman's voice is replicated without her consent to deceive or extort, can be prosecuted under this provision.

Section 66E punishes whoever intentionally captures, publishes or transmits the image of a private area of any person without his or her consent, in circumstances violating that person's privacy.⁴⁵ However, when this section is read in the context of NCII or deepfakes, it creates what this paper terms the *Authenticity Paradox*. In AI-generated intimate imagery, the private area depicted is entirely fabricated -it is not real -while the face of the woman is real. Her privacy is violated at its very core, yet the more completely the image is AI-generated, the less it fits the statutory definition. The provision was designed for real photographs of real bodies; it was never designed for a reality in which a woman's face can be attached to an invented body to humiliate and destroy her.

Sections 67 and 67A punish the publishing or transmitting of obscene or sexually explicit material.⁴⁶ However, the emphasis on words such as "lascivious" and "prurient interest" reveals that this law was conceived as a crime against public morality, not against a woman's autonomy or consent. This is precisely where the law must evolve. The harm of a non-consensual deepfake is not that it offends public sensibility; it is that it strips a real woman of her dignity,

⁴³ The Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).

⁴⁴ *Id.* § 66D.

⁴⁵ *Id.* § 66E.

⁴⁶ *Id.* §§ 67, 67A.

her reputation and her freedom without her knowledge or consent.

The IT Act nowhere defines NCII, deepfakes or AI-enabled abuse, nor has it been amended to include these emerging categories of crime that violate consent and strip away the dignity and autonomy of women. In this respect, it remains a law of a different era, trying inadequately to govern harms it was never designed to address.

2.2.2 The Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) replaced the Indian Penal Code, 1860 with effect from 1 July 2024. While the BNS represents a significant legislative exercise in modernising India's criminal law, it remains, at its core, a codification of traditional crimes, and this is precisely where it fails the victims of AI-enabled gender violence.

Section 75 defines sexual harassment as unwelcome physical contact, a demand or request for sexual favours, showing pornography against the will of a woman, or making sexually coloured remarks.⁴⁷ The provision is grounded entirely in physical and direct acts. It does not contemplate the creation of non-consensual intimate imagery, deepfakes or AI-generated pornography as a form of sexual harassment, even though such content is, in effect, sexual harassment committed in front of millions of people at the same time. The impact of AI-generated sexual content is not confined to bodily integrity alone; it destroys reputation, violates identity, causes severe psychological harm and silences women from public life on a scale that no act of physical harassment could ever match. By limiting itself to the traditional concept of sexual harassment, Section 75 leaves this vast and growing category of harm entirely unaddressed.

Section 77 defines voyeurism as watching or capturing the image of a woman engaging in a private act in circumstances where she would usually expect not to be observed, or disseminating such an image.⁴⁸ The key phrase is “engaging in a private act”. In cases of AI-enabled abuse, however, a woman's face or identity can be extracted from any public image - a professional photograph, a social media post, even a passport-size photograph - and used to generate intimate or sexual content without her knowledge or consent. The victim was never engaged in a private act; she was simply existing in public. Section 77 therefore provides no

⁴⁷ The Bharatiya Nyaya Sanhita, 2023, § 75, No. 45, Acts of Parliament, 2023 (India).

⁴⁸ *Id.* § 77.

remedy to the overwhelming majority of deepfake victims, because the provision was designed for a world where a perpetrator had to physically observe or capture a woman in a private setting. AI has made that requirement irrelevant.

Section 78 punishes stalking, including monitoring a woman's use of the internet or electronic communication.⁴⁹ While this provision can extend to AI-assisted forms of digital surveillance and tracking, it does not address the weaponisation of AI tools to generate harmful content, to impersonate or to extort.

Section 319 deals with cheating by personation.⁵⁰ AI-enabled voice cloning incidents, in which a woman's voice is replicated without her consent to deceive family members or extort money, can be prosecuted under this provision. However, neither the section nor its illustrations refer to AI-enabled impersonation, which leaves the prosecution to stretch the language of a provision drafted in an entirely different technological era.

Section 76 (earlier Section 354B of the IPC) punishes the use of criminal force or assault on a woman with the intention of disrobing her, and Section 77 replaced the voyeurism offence in Section 354C of the IPC.⁵¹ These provisions speak the language of physical proximity and bodily presence. They have no answer to a crime in which the perpetrator is anonymous, geographically boundless and never comes within a thousand miles of the woman he is destroying.

The BNS is the core penal law of India. When the penal law confines itself to traditional categories of crime without acknowledging the new and rapidly evolving landscape of AI-enabled violence, it does not merely fail to punish perpetrators; it actively abandons victims, leaving them without justice, without remedy and without the most basic assurance that the law sees their suffering at all. A criminal law that does not recognise a crime sends a message far more dangerous than silence: it tells every perpetrator that what he is doing is beyond the reach of consequence.

2.2.3 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's core legislation

⁴⁹ *Id.* § 78.

⁵⁰ *Id.* § 319.

⁵¹ *Id.* §§ 76–77.

governing and protecting digital personal data, and it seeks to create a balance between individual privacy rights and lawful business needs. It provides rules and principles on how businesses, companies and intermediaries may collect and use personal data. However, Section 3(c)(i), which explains the applicability of the Act, clearly excludes personal data processed by an individual for any personal or domestic purpose.⁵² This exclusion is a critical flaw in the context of AI-enabled abuse. The overwhelming majority of deepfake perpetrators are private individuals, not corporations. By excluding individuals from its ambit, the DPDP Act does not penalise those individuals who alter or disseminate a woman's personal data through AI tools, and consequently provides no direct remedy to victims of AI-enabled abuse.

However, the DPDP Act defines consent in an extensive and meaningful form, which becomes valuable when we discuss the violation of consent that is central to AI-enabled abuse. Section 6 requires that consent must be free, specific, informed, unconditional and unambiguous, and given through a clear affirmative action.⁵³ This statutory definition of consent gives the judiciary a solid legislative foundation to interpret and apply the concept of consent in cases involving deepfakes, voice cloning and non-consensual intimate imagery, even where the Act itself does not directly penalise the perpetrator.

2.2.4 Consent: The Missing Foundation of the Law

Consent is the common thread in every form of AI-enabled gender violence, but our criminal law does not place it at the centre. Consent is not a general permission; it is given for a specific act, a specific purpose and a specific context. When a woman uploads her photograph on Instagram, she consents to her followers seeing it. She does not consent to her photograph being used in a “nudify” app, being turned into a sexual image, or being shared on a pornographic website. Privacy scholars call this “contextual integrity”: information shared in one context cannot be moved into another context without consent.⁵⁴ Therefore, every stage of deepfake abuse -capturing, creating, sharing and threatening to share -is a separate violation of consent. By the standard of Section 6 of the DPDP Act, a woman's silence, her presence in public or her decision to share a photograph can never be treated as consent to her sexualisation. Other countries have made consent the test: the new English offence asks whether the woman

⁵² The Digital Personal Data Protection Act, 2023, § 3(c)(i), No. 22, Acts of Parliament, 2023 (India).

⁵³ *Id.* § 6(1).

⁵⁴ Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004).

consented to the creation of the image,⁵⁵ and Australia rebuilt its offences on a “consent model” that covers both real and fake sexual material.⁵⁶ With smart glasses, a woman cannot consent to a recording she does not know about. When the law moves from obscenity to consent, the question changes from “does this image offend public morality?” to “did the woman agree?” This puts the woman, and not society’s idea of decency, at the centre of the law.

2.2.5 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

The IT Amendment Rules, 2026, notified on 10 February 2026 and in force from 20 February 2026, mark a turning point in India’s legal response to AI-enabled gender violence.⁵⁷ For the first time in India’s legislative history, AI-generated harmful content has received explicit legal recognition. The Rules define “synthetically generated information” (SGI) as audio, visual or audio-visual content created or altered by AI so that it appears real and is likely to be perceived as indistinguishable from a real person or event. This covers deepfake videos, AI-morphed photographs and cloned audio, but unlike the October 2025 draft, it does not cover synthetic text.⁵⁸

The Rules impose significant obligations on platforms. Platforms that offer AI tools must use technical measures to prevent the creation of unlawful SGI, including non-consensual intimate imagery.⁵⁹ Lawful synthetic content must carry a prominent label, audio content must carry an audio disclosure, and permanent metadata must be embedded where technically possible.⁶⁰ Significant Social Media Intermediaries -platforms with more than fifty lakh registered users in India -must ask users to declare whether their content is synthetic and must verify this declaration through technical measures.⁶¹ Most critically, the takedown time has been reduced: platforms must act on a court or government order within three hours, and must remove

⁵⁵ Sexual Offences Act 2003, c. 42, § 66E (UK).

⁵⁶ Commonwealth, *Parliamentary Debates*, House of Representatives, 5 June 2024 (Mark Dreyfus, Attorney-General) (Second Reading Speech, Criminal Code Amendment (Deepfake Sexual Material) Bill 2024) (Austl.).

⁵⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).

⁵⁸ Aakriti Bansal, *MeitY Notifies New Amendments to IT Rules to Regulate Synthetic Media and Deepfakes*, MediaNama (Feb. 10, 2026), <https://www.medianama.com/2026/02/223-meity-amendments-it-rules-synthetic-media-deepfakes/>.

⁵⁹ IT Amendment Rules, 2026, r. 3(3)(a)(i).

⁶⁰ *Id.* r. 3(3)(a)(ii).

⁶¹ *Id.* r. 4(1A).

intimate or morphed content reported by the victim within two hours.⁶² The Rules also make it clear that platforms which remove such content in good faith do not lose their safe-harbour protection, which encourages swift action without fear of liability.⁶³

However, the IT Amendment Rules, 2026 have significant limitations that this paper must honestly acknowledge. First, the Rules regulate platform conduct; they do not create direct criminal liability for the individual who creates and distributes a deepfake. A man who fabricates a sexual deepfake of a woman and sends it on WhatsApp faces no specific punishment under these Rules. Second, the short takedown windows mean little in practice when most victims in India do not know how to complain to a platform, have no access to legal assistance and receive no response when they report content. Third, the Rules place the burden of action on platforms and victims, not on perpetrators. This is a fundamental inversion of how criminal law should operate.

The Indecent Representation of Women (Prohibition) Act, 1986 prohibits the indecent representation of women in advertisements, publications and similar material, and it is listed among the laws that apply to AI-generated sexual imagery.⁶⁴ However, it was designed for print media and advertisements, and it too is framed around “indecentry” rather than consent.

2.2.6 Conclusion on Indian Statutes: The Problem of Remedial Fragmentation

Taken together, the IT Act, 2000, the BNS, 2023, the DPDP Act, 2023 and the IT Amendment Rules, 2026 form a mosaic of provisions that approach AI-enabled gender violence from different angles, without any single provision comprehensively addressing it. A victim of deepfake abuse must simultaneously invoke Section 66E of the IT Act for privacy violation, Sections 67 and 67A for obscene content, Section 75 of the BNS for sexual harassment, Section 319 for personation and the DPDP Act for consent violation -and she will still find that none of these provisions was written with her specific harm in mind.

This is remedial fragmentation in its most acute form. It does not merely inconvenience victims; it re-traumatises them. Every additional forum, every additional provision and every additional procedural hurdle is another door a woman must knock on while the content that is

⁶² Bansal, *supra* note 58.

⁶³ *Id.*; see also IT Act § 79.

⁶⁴ The Indecent Representation of Women (Prohibition) Act, 1986, §§ 3–4, No. 60, Acts of Parliament, 1986 (India).

destroying her life continues to circulate.

2.3 Judicial Response

Indian courts, particularly the Delhi High Court, have shown more responsiveness than the legislature in addressing AI-enabled gender violence. In *X v. Union of India* (2021), the Delhi High Court directed the removal and de-indexing of a woman's ordinary photographs that had been placed on a pornographic website without her consent, and the prevention of their re-upload, memorably observing that "the internet never sleeps; and the internet never forgets."⁶⁵ In *Mrs. X v. Union of India* (2023), the Court went further, holding that search engines must remove all offending content and not merely specific links, and recommending digital identifiers for victims to prevent re-uploads without fresh court applications.⁶⁶ In *Anil Kapoor v. Simply Life India* (2023) and *Sadhguru Jagadish Vasudev v. Igor Isakov* (2025), the Court granted broad and dynamic injunctions protecting name, image, voice and persona against AI misuse, recognising that freely available AI tools make it possible for anyone to imitate or fabricate a person's identity.⁶⁷ Most recently, in *Kamya Buch v. JIX5A* (2025), the Court extended these tools to protect an ordinary woman by restraining accounts, directing takedown, ordering disclosure of the anonymous perpetrators and protecting the victim's confidentiality in the court record itself.⁶⁸

However, four honest limitations must be acknowledged. First, most of this relief comes from the Delhi High Court through civil suits or writ petitions, which require a lawyer, money, time and physical access to a High Court -resources that most women in small towns and villages simply do not have. Second, the personality rights judgments in *Anil Kapoor* and *Sadhguru* protect the commercial value of a celebrity's identity; an ordinary woman has no brand to protect, and her injury is to her dignity, not her business, which makes these precedents a poor fit for the majority of victims. Third, the relief remains case by case: each woman must start again, prove again, and find the same content on new websites all over again. Fourth, and most critically, these orders concern takedown and disclosure; the perpetrators themselves largely escape consequence, because criminal prosecution follows separately, slowly and, more often than not, not at all. Indian courts have shown the spirit of *Vishaka* -creativity in the face of

⁶⁵ *X*, 2021 SCC OnLine Del 1788.

⁶⁶ *Mrs. X*, 2023 SCC OnLine Del 2361.

⁶⁷ *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914 (India); *Sadhguru Jagadish Vasudev v. Igor Isakov*, 2025 SCC OnLine Del 3804 (India).

⁶⁸ *Kamya Buch v. JIX5A*, 2025 SCC OnLine Del 6428 (India).

legislative silence -but judicial creativity alone cannot substitute for the clear, accessible and enforceable statutory protection that Parliament has so far failed to provide.

The constitutional aspirations of Articles 14, 15 and 21 -equality, special protection for women, dignity and privacy -are vivid and powerful on paper. The statutory framework meant to give those aspirations practical force is fragmented, outdated and silent on the most urgent harms of our time. India's laws speak the language of the twentieth century, while the violence being done to women is being committed in the twenty-first. Closing that gap is not a legislative luxury. It is a constitutional obligation.

3. Comparative Analysis

AI-enabled abuse is not an isolated or domestic crime; it occurs and is facilitated at the international level. Indian women are not alone in facing AI-enabled violence. Like the internet, AI-enabled abuse has no boundaries, as the Grok episode confirms, where different countries took different approaches to deal with the same NCII.⁶⁹ In this globalising world, different countries face similar difficulties in handling digital crime, i.e. the violation of the consent, dignity and autonomy of the individual, the difficulty of catching perpetrators, and the adjudication of crime and punishment of wrongdoers. So India, as part of the global community, can take inspiration and ideas from how other nations are approaching the task of preventing and regulating this faceless crime.

3.1 Legislative Steps Taken by the United Kingdom, the European Union, the United States and Australia: A Case Study for India

3.1.1 United Kingdom

The United Kingdom, through the Online Safety Act 2023, criminalised sharing, or threatening to share, an intimate photograph or film without consent, including deepfakes.⁷⁰ Then, the Data (Use and Access) Act 2025 inserted Sections 66E to 66H into the Sexual Offences Act 2003, which, from 6 February 2026, make it an offence to create, or ask someone to create, a “purported intimate image” of a person without that person’s consent or a reasonable belief in consent.⁷¹ This is an important step that resolves some problems. First, recognition is crucial;

⁶⁹ See *Grok Blocked by Indonesia, Malaysia, supra* note 11.

⁷⁰ Online Safety Act 2023, c. 50, § 188 (UK); Sexual Offences Act 2003 § 66B.

⁷¹ Data (Use and Access) Act 2025, c. 18, § 138 (UK); The Data (Use and Access) Act 2025 (Commencement

recognising an act as a crime is the first step towards preventing it. Second, the UK has taken a step forward by criminalising the creation of NCII before it is shared, and consent, not public morality, becomes the test for purported intimate images. This provides a solution to the Authenticity Paradox, which is one of the limitations of India's IT Act, 2000.

3.1.2 European Union

The European Union has taken the broadest regulatory approach. The EU Artificial Intelligence Act defines a “deep fake” as AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places or events and would falsely appear to a person to be authentic or truthful.⁷² Article 50 requires providers of generative AI systems to mark their output in a machine-readable way so that it can be detected as artificial, and requires those who use AI to create deepfakes to disclose that the content has been artificially generated or manipulated.⁷³ After the Grok incident, the EU amended the AI Act in 2026 to ban “nudifier” AI systems that create sexual images of an identifiable person without consent, as well as AI systems that create child sexual abuse material; this ban applies from 2 December 2026.⁷⁴ The EU Directive on combating violence against women and domestic violence, adopted in May 2024, also requires every member state to criminalise sharing intimate images without consent, including producing, manipulating or altering such images.⁷⁵

3.1.3 United States

The US has no comprehensive law on AI or data protection; its main federal response to intimate image abuse is the TAKE IT DOWN Act, 2025.⁷⁶ It criminalises publishing intimate images of an identifiable person without consent and expressly covers digital forgeries (images created or altered by software, apps or AI). It requires “covered platforms” to set up a clear process through which victims can request removal, and to remove the content within 48 hours;

No. 5) Regulations 2026, SI 2026/31 (UK).

⁷² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689), art. 3(60).

⁷³ *Id.* art. 50.

⁷⁴ Press Release, Eur. Parl., Artificial Intelligence Act: Delayed Application, Ban on Nudifier Apps (Mar. 26, 2026), <https://www.europarl.europa.eu/news/en/press-room/20260323IPR38829/artificial-intelligence-act-delayed-application-ban-on-nudifier-apps>; *European Parliament Approves AI Act Amendments, ‘Nudifier’ Ban*, Sofia Globe (June 16, 2026), <https://sofiaglobe.com/2026/06/16/european-parliament-approves-ai-act-amendments-nudifier-ban/>.

⁷⁵ Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, 2024 O.J. (L 1385), art. 5.

⁷⁶ TAKE IT DOWN Act, Pub. L. No. 119-12 (2025) (U.S.).

a violation attracts civil penalties of up to \$53,088 per violation.⁷⁷ However, it only targets the publication of NCII, not its creation, which the UK has addressed directly.

3.1.4 Australia

Australia's Criminal Code Amendment (Deepfake Sexual Material) Act 2024 criminalises sharing sexual material depicting an adult without consent, whether real or AI-generated, punishable by up to six years' imprisonment, and up to seven years where the person who shares it also created it.⁷⁸ Australia's Online Safety Act 2021 created the eSafety Commissioner, an independent regulator with the power to receive complaints of image-based abuse, including digitally altered images, and to order platforms to remove such material within 24 hours, backed by civil penalties.⁷⁹

3.2 Lessons for India

From these countries, India can take inspiration to make a comprehensive statute. First, it should criminalise both the creation and the sharing of AI-enabled abuse. Second, it should shift its focus from public morality to the consent of the individual. Third, it should regulate the tools and not only the users. India's 2026 Rules already require platforms to prevent unlawful SGI, but neither the Rules nor the DPDP Act, 2023 ban stand-alone nudify apps. When an AI tool like Grok can produce abuse on demand, removing images afterwards is not enough. Fourth, India should give the victim one door to knock on. Like Australia's eSafety Commissioner, a single public body should receive complaints, contact platforms, issue removal notices and track outcomes. This would remove the difficulty Indian women face in dealing separately with platforms, the police, the courts and the Data Protection Board.

3.3 Smart Glasses: An Opportunity for India

India can also set an example by making foolproof legislation on smart glasses, because no jurisdiction has solved this problem yet. All five countries, including India, rely on older voyeurism laws tied to a private act; in the UK, for example, there is no specific law against

⁷⁷ Fed. Trade Comm'n, *Complying with the Take It Down Act* (May 2026), <https://www.ftc.gov/business-guidance/resources/complying-take-it-down-act>.

⁷⁸ Criminal Code Amendment (Deepfake Sexual Material) Act 2024 (Cth) (Austl.); Dreyfus, Second Reading Speech, *supra* note 56.

⁷⁹ Online Safety Act 2021 (Cth) (Austl.).

filming a person in a public place without consent.⁸⁰ The industry is experimenting with its own responses. HTC's glasses stop recording if someone nearby says "stop recording",⁸¹ and Meta has launched new glasses without a camera that only respond to voice.⁸² But these are voluntary steps by companies. In this area of smart glasses, where very little has been done at the global level, India can become a global leader by making legal rules for their use that maintain the dignity and autonomy of women.

4. Rethinking: The Way Forward

The previous chapters show that AI has created new weapons against women, that the harm caused by these weapons violates their fundamental rights, and that Indian law answers this harm with scattered provisions made for a different era. India therefore needs to rethink its law with the consent and dignity of women at the centre. The following steps can be taken.

First, a specific offence based on consent. Parliament should make a specific offence of AI-enabled sexual abuse, either in the BNS or in a separate law. It should punish creating, asking someone to create, sharing and threatening to share a fake intimate image, video or audio of a person without consent, as the UK now does.⁸³ Consent should have the same meaning as in Section 6 of the DPDP Act, and the law should clearly say that posting a photo online is not consent to its sexualisation. The offence should not depend on a "private act" or a real "private area"; it should be enough that the material shows, or appears to show, the person in a sexual manner. This would solve the Authenticity Paradox. Section 66E of the IT Act should also cover fake ("purported") images, and Section 66C should clearly include a person's face and voice as a unique identification feature.

Second, regulate the tools, not only the users. Punishing offenders after the harm is not enough. Like the EU, India should ban AI tools that create sexual images of real people without consent unless they have effective safeguards.⁸⁴ AI companies should be required to block prompts that ask to undress or sexualise real people, and the Government should use its power under Section

⁸⁰ *Women Filmed Secretly*, *supra* note 22.

⁸¹ *HTC Challenges Meta for the US Smart Glasses Market with Vive Eagle*, Android Authority (Sept. 2026), <https://www.androidauthority.com/htc-vive-eagle-us-3706492/>.

⁸² *Meta Releases New 'Audio-Only' Glasses to Combat Privacy Concerns*, BGR (Sept. 2026), <https://www.bgr.com/2267868/meta-smart-glasses-audio-only-no-camera/>.

⁸³ See Sexual Offences Act 2003 §§ 66E–66F.

⁸⁴ See Eur. Parl. Press Release, *supra* note 74.

69A of the IT Act to block nudity websites and apps.⁸⁵ No company should be allowed to make the creation of such images a “premium service”.

Third, one door for every victim. India should create an independent Digital Safety Commissioner, like Australia’s eSafety Commissioner.⁸⁶ Victims should be able to complain to it in their own language through the National Cyber Crime Reporting Portal or the 1930 helpline.⁸⁷ It should order platforms to remove content, track whether they comply, and use the system suggested by the Delhi High Court in *Mrs. X*, where the victim gets a unique token and platforms automatically remove re-uploads of the same content.⁸⁸ In this way, the victim knocks on one door, and the State knocks on the other doors for her.

Fourth, clear rules for smart glasses. India can lead the world here. Smart glasses should have a recording light that cannot be covered or switched off, and the camera should stop working if the light is blocked. People nearby should be able to stop the recording. Face recognition of strangers through such glasses should be banned, because the I-XRAY experiment shows how easily it can be misused.⁸⁹ Recording should be prohibited in washrooms, changing rooms, hospitals, gyms and hostels, and secretly recording a woman and posting the video for profit or humiliation should be an offence even if it was recorded in a public place. Footage of bystanders should not be used to train AI without their consent.

Fifth, amend the DPDP Act. The exemption for personal or domestic use should not apply when a person publishes another person’s data or uses it to harass, humiliate or extort her.⁹⁰ Uploading a deepfake on a website watched by millions is not a “personal or domestic” purpose.

Sixth, a victim-friendly justice process. The identity of victims should be protected as it is for victims of sexual offences under Section 72 of the BNS, and their details should be removed from court records, as was done in *Kamya Buch*.⁹¹ The police should register a zero FIR or an e-FIR, as Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023 allows.⁹² Every district

⁸⁵ See IT Act § 69A.

⁸⁶ See Online Safety Act 2021 (Cth).

⁸⁷ Ministry of Home Affs., *National Cyber Crime Reporting Portal*, <https://cybercrime.gov.in> (last visited Oct. 2, 2026).

⁸⁸ *Mrs. X*, 2023 SCC OnLine Del 2361.

⁸⁹ Koetsier, *supra* note 26.

⁹⁰ See DPDP Act § 3(c)(i).

⁹¹ BNS § 72; *Kamya Buch*, 2025 SCC OnLine Del 6428.

⁹² The Bharatiya Nagarik Suraksha Sanhita, 2023, § 173, No. 46, Acts of Parliament, 2023 (India).

should have trained women officers in its cyber cell, and victims should get free legal aid and compensation. Police officers and judges should be trained to understand deepfakes, so that no woman is told that “it is only a fake picture”.

Seventh, awareness and inclusion. Families should be made aware that they must verify unusual requests for money through a video call before paying, as the Hyderabad police have advised.⁹³ Schools and colleges should teach digital consent, and more women should be included in AI development so that the people who build these tools also include the people most harmed by their misuse.

Conclusion

Until AI came into existence, intelligence was a virtue of humankind. Humans created AI, and some of them turned it into a weapon against women. This paper has shown that deepfakes, voice cloning and sextortion, and smart glasses can harm a woman’s dignity, privacy and freedom without her knowledge and without anyone touching her. This harm is sexual, psychological, social and economic, and it silences women and pushes them out of public life.

The Constitution promises equality, dignity and privacy to every woman, but the statutes do not deliver that promise. The IT Act suffers from the Authenticity Paradox and the language of obscenity; the BNS is tied to physical acts and private places; the DPDP Act excludes individual perpetrators; and the IT Amendment Rules, 2026, though a turning point, regulate platforms rather than punish offenders. The courts have shown creativity, but their relief is costly, case by case and limited mostly to takedown. As a result, a woman has to knock on many doors while the content destroying her life continues to spread.

Other countries have started to act: the UK has criminalised the creation of fake intimate images, the EU has banned nudifier apps, the US has made platforms remove such content within 48 hours, and Australia has given victims a single regulator. India should learn from them, make consent the centre of its law, regulate AI tools and smart glasses, and give every victim one door to knock on. In the area of smart glasses, where no country has a complete answer, India can become a global leader. Weaponised intelligence must be met with intelligent law, and closing this gap is not a choice for India but a constitutional obligation.

⁹³ *Hyderabad Woman Loses Rs 1.97 Lakh in AI Voice Scam*, Telangana Trib. (Mar. 2025), <https://www.telanganatribune.com/hyderabad-woman-loses-rs-1-97-lakh-in-ai-voice-scam/>.

Bibliography

Constitution and Statutes (India)

The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).

The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

The Constitution of India, 1950.

The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

The Indecent Representation of Women (Prohibition) Act, 1986, No. 60, Acts of Parliament, 1986 (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).

The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

Cases

Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914 (India).

Bartone v. Meta Platforms, Inc., No. 3:26-cv-01897 (N.D. Cal. filed Mar. 2026) (U.S.).

Francis Coralie Mullin v. Adm'r, Union Territory of Delhi, (1981) 1 SCC 608 (India).

Joseph Shine v. Union of India, (2019) 3 SCC 39 (India).

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

Kamya Buch v. JIX5A, 2025 SCC OnLine Del 6428 (India).

Mrs. X v. Union of India, 2023 SCC OnLine Del 2361 (India).

Sadhguru Jagadish Vasudev v. Igor Isakov, 2025 SCC OnLine Del 3804 (India).

Vishaka v. State of Rajasthan, (1997) 6 SCC 241 (India).

X v. Union of India, 2021 SCC OnLine Del 1788 (India).

Foreign Legislation and International Instruments

Criminal Code Amendment (Deepfake Sexual Material) Act 2024 (Cth) (Austl.).

The Data (Use and Access) Act 2025 (Commencement No. 5) Regulations 2026, SI 2026/31 (UK).

Data (Use and Access) Act 2025, c. 18 (UK).

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, 2024 O.J. (L 1385).

Online Safety Act 2021 (Cth) (Austl.).

Online Safety Act 2023, c. 50 (UK).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).

Sexual Offences Act 2003, c. 42 (UK).

TAKE IT DOWN Act, Pub. L. No. 119-12 (2025) (U.S.).

Reports and Official Documents

Commonwealth, *Parliamentary Debates*, House of Representatives, 5 June 2024 (Mark Dreyfus, Attorney-General) (Second Reading Speech, Criminal Code Amendment (Deepfake Sexual Material) Bill 2024) (Austl.).

Fed. Trade Comm'n, *Complying with the Take It Down Act* (May 2026).

Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeprace, Sept. 2019).

McAfee, *Beware the Artificial Impostor: A McAfee Cybersecurity Artificial Intelligence Report* (May 2023).

Nat'l Crime Records Bureau, Ministry of Home Affs., *Crime in India 2023* (2025).

Office of the U.N. High Comm'r for Hum. Rts., *Call for Inputs: 2026 Thematic Report on Gender Equality in the Digital Space and Age* (2025).

Press Release, Eur. Parl., Artificial Intelligence Act: Delayed Application, Ban on Nudifier Apps (Mar. 26, 2026).

Security Hero, *2023 State of Deepfakes: Realities, Threats, and Impact* (2023).

U.S. Dep't of Homeland Sec., Sci. & Tech. Directorate, *S&T Digital Forgeries Report: Impacts*

of Generative Artificial Intelligence (Fiscal Year 2024 Report to Congress) (Jan. 17, 2025).

UN Women, *FAQs: AI-Powered Online Abuse: How AI Is Amplifying Violence Against Women and What Can Stop It* (Nov. 2025).

UN Women, *How AI Is Exacerbating Technology-Facilitated Violence Against Women and Girls* (2026).

World Econ. F., *Global Gender Gap Report 2023* (June 2023).

Articles

Clare McGlynn & Erika Rackley, *Image-Based Sexual Abuse*, 37 Oxford J. Legal Stud. 534 (2017).

Clare McGlynn et al., *'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse*, 30 Soc. & Legal Stud. 541 (2021).

Designed for Privacy? The Bartone v. Meta Litigation over AI Smart Glasses, MediaLaws (July 2026).

Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004).

Ian J. Goodfellow et al., *Generative Adversarial Networks* (2014).

Smart Glasses and Privacy: Wearable Surveillance and Disclosure Issues, Nat'l L. Rev. (Apr. 2026).

News Reports and Online Sources

A Woman from Hyderabad Loses 1.4 Lakh Rupees in an AI Scam, IndiaAI (2023).

Aakriti Bansal, *MeitY Notifies New Amendments to IT Rules to Regulate Synthetic Media and Deepfakes*, MediaNama (Feb. 10, 2026).

Aleesha Sam, *Social Media Platform X 'Admits' Mistake over Grok Obscenity; 3,500 Posts Blocked, 600 Accounts Deleted After Govt Notice*, Free Press J. (Jan. 11, 2026).

England and Wales Ban Meta Glasses from Courtrooms, Engadget (Aug. 2026).

European Parliament Approves AI Act Amendments, 'Nudifier' Ban, Sofia Globe (June 16, 2026).

Grok Blocked in Indonesia and Malaysia as UK Launches Probe over Sexualised Images, ABC News (Austl.) (Jan. 12, 2026).

Harvard Students Used Meta's Smart Glasses and AI to Get Private Info from People's Photos, Bos. Globe (Oct. 4, 2024).

HTC Challenges Meta for the US Smart Glasses Market with Vive Eagle, Android Authority (Sept. 2026).

Hyderabad Woman Falls Victim to AI Voice Scam, Loses Rs 1.97 Lakh, Hans India (Mar. 2025).

Hyderabad Woman Loses Rs 1.97 Lakh in AI Voice Scam, Telangana Trib. (Mar. 2025).

Indonesia Temporarily Blocks Access to Grok over Sexualised Images, Reuters (Jan. 10, 2026), reprinted in ThePrint.

IT Act Toothless Against Deepfakes? NCW Seeks Review of Laggard Laws as Women Face More AI-Driven Abuse, ThePrint (Nov. 2025).

John Koetsier, Meta's Ray-Ban Smart Glasses Used to Instantly Dox Strangers in Public, Thanks to AI and Facial Recognition, Forbes (Oct. 3, 2024).

Meta Ray-Bans Banned in UK Pubs and Theatres and the Smart Glasses Era Could Be Doomed, Stuff (Aug. 2026).

Meta Releases New 'Audio-Only' Glasses to Combat Privacy Concerns, BGR (Sept. 2026).

Meta Sued over AI Smart Glasses' Privacy Concerns, After Workers Reviewed Nudity, Sex, and Other Footage, TechCrunch (Mar. 5, 2026).

Ministry of Home Affs., *National Cyber Crime Reporting Portal*.

Musk's Grok Blocked by Indonesia, Malaysia over Sexualized Images in World First, CNN (Jan. 12, 2026).

Shares of Ray-Ban Maker EssilorLuxottica Jump 6% on Reported Meta Stake in AI Push, CNBC (July 9, 2025).

Women Filmed Secretly for Social Media Content – and Then Harassed Online, Herald Times (Jan. 25, 2026) (reporting a BBC News investigation).