THE LAWWAY WITH LAWYERS JOURNAL

Website: www.the lawway with lawyers.com

VOLUME:-38 ISSUE NO:- 38 , SEPTEMBER 20, 2026

ISSN (ONLINE):- 2584-1106

Email: thelawwaywithelawyers@gmail.com

Digital Number : 2025-23534643

CC BY-NC-SA

Authored By:- Bhavesh Gautam

Amity law School, Amity University Patna

DEEPFAKE TECHNOLOGY AND THE LAW: ADDRESSING EMERGING THREATS IN THE DIGITAL ERA

Abstract

Deepfakes, meaning AI-generated or altered audio and video that convincingly imitate real people, have moved within a few years from an internet curiosity to a mainstream legal problem. This paper examines how law is responding, with India as its main focus and the United States, the European Union, the United Kingdom, China, South Korea and Denmark as comparators. It identifies five groups of harm: non-consensual intimate imagery, fraud, political manipulation, violation of personality and dignity, and the erosion of trust in evidence. It then assesses India's layered response: older provisions of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023; the IT Rules amendment in force since 20 February 2026, which

introduces labelling and two- to three-hour takedown deadlines; and a growing line of High Court personality-rights orders. The paper argues that these measures are a meaningful start but remain dependent on subordinate rules and interim relief, and it highlights gaps in attribution, jurisdiction, free-speech safeguards, evidence and victim access. It concludes with recommendations for a dedicated statute, a civil remedy for ordinary victims, clear exceptions for satire and journalism, stronger forensic and police capacity, and public awareness.

Keywords: deepfakes, synthetically generated information, IT Rules 2026, personality rights, intermediary liability, AI regulation, India

1. Introduction

Imagine opening your phone one morning to find a video of yourself saying or doing something you never said or did. The face is yours, the voice is yours, and strangers are already sharing it. Within hours, people who know you start asking whether it is real. This is not a distant scenario. In November 2023, a fabricated video of actor Rashmika Mandanna went viral in India, prompting a public outcry and a police investigation, and it became many Indians' first real encounter with the word "deepfake". Since then, the problem has only grown more personal and more common.

Deepfakes sit at an uncomfortable meeting point between technology, law and human dignity. They can be used to humiliate a classmate, to impersonate a company executive and authorise a fraudulent transfer, to put false words in a politician's mouth days before an election, or to market a product using a celebrity's face without their knowledge. Each of these harms touches a different branch of law: criminal law, privacy, intellectual property, defamation, electoral law and intermediary liability. No single statute was written with them in mind.

This paper asks four questions:

1. What is the nature of the harm that deepfakes cause, and to whom?
2. How far does India's existing legal framework, including its most recent amendments, address that harm?
3. How have other major jurisdictions responded, and what can India learn from them?

4. What gaps remain, and what reforms would protect people without choking legitimate speech and innovation?

Scope and method. The paper uses a doctrinal and comparative approach. It draws on statutes, rules, court orders and legal commentary, with India as the primary focus and the United States, the European Union and a few other countries as comparators. Because this field moves quickly, the discussion reflects the position as of November 2026; some rules cited here were notified or came into force only in the past year, and readers should verify the latest text before relying on any provision.

2. Understanding Deepfakes: The Technology Behind the Illusion

A deepfake is synthetic media, a video, image or audio clip, in which a person's face, body or voice has been generated or altered by artificial intelligence so convincingly that it appears real. The word itself is a blend of "deep learning" and "fake", and it entered everyday vocabulary in late 2017, when an anonymous online user began posting face-swapped videos made with open-source machine-learning tools.

To see why the law struggles with deepfakes, it helps to understand how they are made. Three families of technique matter most.

- **Autoencoders and face-swapping.** An autoencoder learns to compress thousands of images of a face into a compact code and then rebuild them. Train two such systems on two different people, swap their decoders, and one person's expressions can be painted onto another person's face.
- **Generative Adversarial Networks (GANs).** Introduced by Ian Goodfellow and colleagues in 2014, a GAN pits two neural networks against each other: a generator that produces fakes and a discriminator that tries to catch them. Each round makes the generator better, until the discriminator can no longer tell the difference. This adversarial design is precisely why detection tools are always playing catch-up.
- **Diffusion models and voice cloning.** Newer image and video generators work by gradually turning random noise into a coherent picture, guided by a text prompt.

Voice-cloning systems can now reproduce a person's speech from a short sample of recorded audio, including their accent and rhythm.

The most important change over the last few years is not the quality of the fakes but the cost of making them. In the early days, a convincing deepfake needed technical skill, powerful hardware and many hours. Today, phone apps and web tools can produce a passable fake in minutes, often for free. That shift, from a specialist's craft to a mass-market tool, is what turns deepfakes from a curiosity into a legal problem. When anyone can fabricate a person's likeness, the harms are no longer rare events; they become an everyday risk for ordinary people, not only for celebrities and politicians.

It is also worth remembering that the technology is not inherently malicious. The same techniques power film dubbing, voice restoration for people who have lost their speech, accessibility tools, education and satire. A sensible legal response therefore cannot simply ban the technology. It has to separate harmful uses, such as deception, fraud, harassment and non-consensual sexual imagery, from legitimate creative and expressive ones.

3. The Threat Landscape: Who Gets Hurt, and How

It is tempting to think of deepfakes as a problem for famous people. The evidence points the other way: the people most often harmed are ordinary individuals, and women and girls above all. The harms fall into five broad groups.

Non-consensual intimate imagery.

This is the oldest and still the most damaging use. Early research, such as the Deeptrace report of 2019, found that the great majority of deepfake videos online were pornographic and that almost all of them targeted women. The pattern has only intensified with "nudify" apps that strip clothing from an ordinary photograph in seconds. South Korea's experience in 2024 is a warning for every country: police there handled more than 800 deepfake sex-crime cases in a single year, and reports described most offenders as teenage boys targeting classmates and acquaintances,

sometimes as a "prank". For the victim, it hardly matters that the image is fake. The shame, anxiety and social damage are real, and so is the fear that the image will resurface years later.

Fraud and impersonation.

Voice and video cloning have given scammers a powerful new tool. In early 2024, an employee of the engineering firm Arup in Hong Kong was reportedly tricked into transferring about US$25 million after joining a video call in which the "colleagues" and the "chief financial officer" were all deepfakes. Closer to home, Indian users are routinely targeted by fake videos of well-known business leaders and actors endorsing investment schemes, and by cloned voices of relatives pleading for urgent money. These scams work because they exploit trust rather than technical weakness; a familiar face or voice switches off our caution.

Political manipulation and public trust.

Deepfakes can be released at the worst possible moment, when there is no time to debunk them. Two examples show the range. In 2023, a fabricated audio clip circulated in the final days of Slovakia's parliamentary election, and in January 2024, a cloned voice of US President Joe Biden was used in robocalls urging voters in New Hampshire to stay home from a primary. India's 2024 general election also saw AI-generated clips of film stars appearing to criticise or endorse political leaders. Even when such content is quickly exposed, it can leave a residue of doubt.

Violation of personality and dignity.

A person's face and voice are part of their identity, and often their livelihood. Actors, singers, sportspeople, journalists and spiritual leaders have found their likeness used to sell products, power fake chatbots, or appear in obscene videos. In the last year alone, the Delhi and Bombay High Courts have granted interim protection to a long list of public figures, including Aishwarya Rai Bachchan, Abhishek Bachchan, Ajay Devgn, Kajol, Akshay Kumar and others.

Damage to evidence and the truth itself.

The subtlest harm may be the most far-reaching. Once people know that any video can be faked, a guilty person can claim that a real recording is a deepfake. Legal scholars Robert Chesney and Danielle Citron called this the "liar's dividend". Courts depend on photographs, recordings and call logs. If every piece of digital evidence can be disputed as synthetic, the burden on judges, forensic experts and victims grows heavier, and the cost of proving the truth rises.

Taken together, these harms share a common feature: they hit hardest where the victim has the least power to respond. A teenager cannot hire a forensics lab. A small business cannot easily trace an overseas scammer. This imbalance is central to the legal question, because the law's task is not only to punish wrongdoers but to give ordinary people a fast, affordable way to protect themselves.

4. The Indian Legal Framework

India has no single "Deepfake Act". Instead, protection comes from three layers that have been stitched together over time: older criminal and civil laws applied to new facts, a fresh set of platform rules aimed squarely at synthetic media, and a growing body of court orders on personality rights.

Existing laws applied to deepfakes.

Until recently, a victim had to fit a deepfake into provisions drafted for other wrongs.

- *Information Technology Act, 2000.* Section 66C (identity theft) and section 66D (cheating by personation using a computer resource) fit impersonation and fraud. Section 66E punishes capturing or publishing a person's private image in violation of privacy. Sections

67 and 67A cover obscene and sexually explicit electronic material, and section 67B covers child sexual abuse material. Section 69A lets the government direct blocking of content, and section 79 gives intermediaries "safe harbour" from liability for user content, provided they follow due diligence.

- *Bharatiya Nyaya Sanhita, 2023.* Sections 318 and 319 (cheating and cheating by personation) may apply where a deepfake is used to defraud. Depending on the facts, offences such as forgery to harm reputation (section 336), voyeurism (section 77), insulting the modesty of a woman (section 79), defamation (section 356) and criminal intimidation (section 351) may also be invoked.
- *Constitutional and data-protection law.* Since *Justice K.S. Puttaswamy v. Union of India* (2017), privacy is a fundamental right under Article 21, which supplies the constitutional basis for challenging non-consensual use of a person's identity. The Digital Personal Data Protection Act, 2023 adds a consent-based framework for processing personal data, which is relevant because a deepfake necessarily processes a real person's face or voice.

This patchwork works, but only awkwardly. None of these provisions mentions synthetic media, none sets a response time for the victim, and the burden of proving that a fake image "is" the person falls on the complainant.

The IT Rules amendment of 2026

The most important development is the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and in force from 20 February 2026. For the first time, Indian rules define "synthetically generated information": audio, visual or audio-visual content created or altered by computer so that it appears real. Routine editing, good-faith documents and accessibility uses are excluded, and AI-generated text is not covered.

The Rules place two sets of duties on intermediaries:

- Services that let users create synthetic content must use reasonable technical measures to prevent unlawful material, such as non-consensual intimate imagery, false documents or

content that deceptively shows a real person, and must label all other synthetic content and embed permanent metadata or a unique identifier where technically feasible.

- Significant social media intermediaries, meaning platforms with at least 50 lakh registered users in India, must ask users to declare whether content is synthetic, verify the declaration with technical measures, and label the content. A platform that knowingly fails to act risks losing its safe harbour under section 79.

The amendment also shortens takedown deadlines sharply:

Situation	Earlier deadline	Current deadline
Unlawful content, on a court order or reasoned government notice	36 hours	3 hours
Intimate, sexual or impersonating images (including morphed images), on the victim's complaint	24 hours	2 hours
Resolving a user grievance	15 days	7 days

The same source notes that, in April 2026, MeitY consulted on a further draft amendment, so this area is still moving.

Personality rights:

the courts step in. While the rules were being written, High Courts did what legislatures had not. In *Anil Kapoor v. Simply Life India* (Delhi High Court, 2023), the court restrained the misuse of an actor's name, image, voice and likeness, including through AI. Since 2025 the pace has quickened. The Delhi High Court has granted interim protection to Sri Sri Ravi Shankar against deepfake and AI-generated content, and to Ajay Devgn, ordering the removal of obscene deepfake videos, while the Bombay High Court, in an order for Akshay Kumar, described the misuse as "truly alarming". In the *Raj Shamani* case, the Delhi High Court drew a useful line between commercial exploitation of identity, which can be stopped, and satire or parody, which remains protected.

These orders show courts reaching for a flexible tool, usually through "John Doe" injunctions that bind unknown future offenders. But they are interim, expensive and mostly sought by well-known people. A schoolgirl or a small shopkeeper has neither the means nor the time to file a commercial suit in a High Court.

An honest assessment.

The 2026 Rules are a real step forward. They name the problem, they put duties on the platforms best placed to act, and they give victims of intimate deepfakes a two-hour clock. But four weaknesses stand out.

1. *Rules, not a statute.* The regime sits in subordinate legislation and works mainly through the threat of losing safe harbour. It creates no direct civil right for the victim and no dedicated criminal offence for creating a harmful deepfake.
2. *Narrow coverage.* Text is excluded, and labelling duties rest on technical measures, such as metadata, that a determined bad actor can strip out or avoid by using offshore tools.
3. *Over-removal risk.* A three-hour deadline gives platforms little time to judge context. The sensible response for a platform is to delete first and ask questions later, which can sweep up satire, journalism and political criticism. This tension echoes the concern in *Shreya Singhal v. Union of India* (2015), where the Supreme Court insisted that takedown duties be tied to court or government orders and not to private complaints alone.
4. *Uneven access to justice.* The fastest remedies still depend on awareness and on a functioning grievance mechanism, which many victims, especially in smaller towns, do not know how to use.

5. Global Approaches: What Other Countries Are Doing

No country has found a perfect answer, but their experiments reveal four distinct strategies: criminalise the worst conduct, force platforms to act quickly, require transparency labels, or give individuals a property-like right over their own likeness. The table below summarises the main instruments as of November 2026.

Jurisdiction	Main instrument	Core approach	Status
United States	TAKE IT DOWN Act (2025)	Crime to publish non-consensual intimate imagery, including AI deepfakes; platforms must remove it within 48 hours of a valid request	Signed 19 May 2025; platform duties enforced by the FTC from 19 May 2026
European Union	AI Act, Article 50	Deployers must disclose deepfakes; providers must mark synthetic output	Applies from 2 August 2026; machine-readable marking for existing systems deferred to 2 December 2026
United Kingdom	Data (Use and Access) Act 2025 and Online Safety Act 2023	Criminalises sharing and, since 2026, creating or requesting sexually explicit deepfakes of adults	Creation offence in force 6 February 2026
China	Deep Synthesis Provisions and AI Labelling Measures	State-supervised duty to label AI content visibly and in metadata	Labelling Measures in force 1 September 2025
South Korea	Sexual crimes punishment law	Criminalises making, distributing, possessing and viewing sexual deepfakes	Up to 7 years for production or distribution; up to 3

Jurisdiction	Main instrument	Core approach	Status
	amendments (2024)		years for possession or viewing
Denmark	Copyright Act amendment, bill L 49	Treats a person's face and voice as protected, so unauthorised realistic imitations can be taken down	Bill introduced 8 October 2026; hoped to take effect early 2027
India	IT Rules amendment 2026	Labelling and metadata duties, user declarations, 2 to 3 hour takedowns	In force 20 February 2026

The United States has moved fastest on the most harmful category. The TAKE IT DOWN Act is the first federal law to tackle intimate deepfakes, and its platform obligations have been enforceable since 19 May 2026. Beyond it, several states, including California, Texas and Illinois, have their own deepfake statutes, especially on intimate imagery and election content. Free-speech groups warn that the 48-hour clock invites over-removal, particularly by smaller platforms that lack moderation teams.

The European Union takes a transparency-first approach. Under Article 50 of the AI Act, anyone who deploys a deepfake must disclose that it is artificially generated, with a lighter duty for evidently artistic or satirical works. Breaches can attract fines of up to 15 million euros or 3 per cent of worldwide turnover. Separately, an EU directive on violence against women requires member states to criminalise creating and sharing sexually explicit manipulated material by 14 June 2027, and France already bars sharing AI-generated images or audio of someone without consent unless the artificial nature is obvious or disclosed.

The United Kingdom has been steadily closing gaps in criminal law. Sharing intimate deepfakes became an offence under the Online Safety Act 2023, and the creation offence followed in

February 2026. The Government has also announced plans to require platforms to remove intimate images within 48 hours.

China relies on administrative control: providers must label AI content both visibly and in embedded metadata, and regulators supervise compliance. It is the most thorough labelling regime in the world, but it rests on a degree of state oversight that would be hard to transplant into a rights-based constitutional democracy.

South Korea offers a sobering lesson on how quickly things can go wrong, and how far a legislature will go in response. After the Telegram-based deepfake scandals of 2024, it criminalised not just making and distributing sexual deepfakes but also knowingly possessing or viewing them.

Denmark is the boldest experiment. Rather than creating a new offence, it proposes to use copyright law to give individuals a legal handle over realistic imitations of their face and voice, with exceptions for satire, parody and criticism. The bill is still before Parliament, and commentators question whether copyright is the right home for what is really a personality right.

What India can learn. Four lessons emerge. First, speed matters most for intimate imagery, and India's two-hour deadline is among the strictest in the world, so the real challenge is making it work in practice. Second, transparency labels help but cannot stand alone, because they only catch honest actors. Third, criminal law should target creation and threats to share, as the UK has done, rather than only distribution. Fourth, any right over one's likeness, whether through copyright or personality rights, needs clear carve-outs for satire, news and criticism so that it does not become a tool of censorship.

6. Gaps and Challenges: Why the Law Struggles to Keep Up

Even the best-drafted law faces hard practical limits when the harm is created by software, spreads across borders and can be copied in seconds. Six challenges deserve attention.

Finding the person responsible.

Most deepfakes are posted anonymously, often from accounts that can be created in minutes and abandoned just as fast. Tracing a creator may require help from foreign platforms, VPN logs or messaging apps that do not cooperate. In practice, a victim can often get the content removed from one site, only to see it reappear on three others. Removal and accountability are two different things, and the law has been far better at the first than the second.

Borders and jurisdiction.

A deepfake made in one country, hosted in another and viewed in a third raises awkward questions: whose law applies, and who enforces it? Indian courts can order Indian platforms to act, but offshore tools and websites are harder to reach. Mutual legal assistance treaties are slow, and a takedown measured in hours cannot depend on a process measured in months. This is why the Danish and EU approaches stress platform duties, since platforms are the one point in the chain that regulators can realistically reach.

The detection arms race.

Tools that spot deepfakes improve, but so do the generators, and the adversarial design of GANs means each advance in detection can be used to train a better fake. Watermarks and metadata, the backbone of labelling laws, are useful but fragile; they can be cropped, compressed away or never added by an offshore tool. Policy that depends on perfect detection will always lag behind the technology.

Balancing speech and safety.

Deepfakes are not always malicious. Satire, parody, political cartoons and film all use imitation. Article 19(1)(a) of the Indian Constitution protects freedom of speech, and any restriction must fit within the reasonable restrictions of Article 19(2). Rules that push platforms to delete within

hours, backed by the threat of losing legal immunity, can lead to cautious over-removal. The Delhi High Court's distinction between exploitation and parody in the *Raj Shamani* case is a helpful model, but it must be turned into clear statutory language, not left to case-by-case judgment.

Proof in court.

The Bharatiya Sakshya Adhiniyam, 2023 recognises electronic records, but courts still lack settled standards for authenticating audio and video when forgery is cheap. The "liar's dividend" means the accused may simply claim that genuine evidence is fake. Courts will need access to trained forensic examiners, clear protocols for expert testimony and, in time, guidance on how much weight to give detection software.

Reaching the people who most need help.

Laws are only as good as the victim's ability to use them. A young woman whose morphed image is circulating in her college WhatsApp group needs three things quickly: someone who believes her, a simple way to report it, and a fast removal. In many cases she gets none of these. Grievance officers can be hard to find, police stations may not understand the offence, and the stigma attached to intimate imagery discourages reporting. A technically perfect rule that victims do not know about will not protect anyone.

7. Recommendations: A Balanced Way Forward

The aim of reform should be simple to state and hard to achieve: protect people from real harm quickly, without handing anyone a switch that silences legitimate expression. The recommendations below are grouped by who has to act.

For Parliament: put the core protections in a statute.

1. Enact a clear statutory definition of a harmful deepfake and create specific offences for creating, requesting or threatening to share sexually explicit synthetic images without consent, following the UK's lead in punishing creation and not only circulation. Offences involving children should carry heavier penalties and no consent defence.
2. Create a direct civil remedy, so that a victim can seek an injunction, damages and an order for the removal of copies without having to prove a separate criminal offence first. This would extend personality-rights protection beyond celebrities to ordinary people.
3. Write express exceptions for satire, parody, journalism, research, education and political criticism, with the burden on the person seeking removal to show actual harm, deception or lack of consent.
4. Treat deepfake-enabled fraud and election manipulation as aggravated forms of existing offences, with sentencing guidance that reflects the scale and speed of the harm.

For regulators and platforms: make speed and fairness work together.

1. Keep short deadlines for intimate imagery, where delay causes irreversible harm, but allow a slightly longer, reasoned process for contested political or satirical content, with a quick right of appeal and restoration if content is wrongly removed.
2. Require platforms to publish transparency reports on synthetic-content complaints, takedown times and error rates, so that the public and the courts can judge whether the rules are working.
3. Mandate hash-matching or similar tools so that once an intimate deepfake is removed, identical copies are blocked from being re-uploaded, as the US law also expects.
4. Adopt interoperable provenance standards, such as content credentials that travel with a file, and treat labelling as one layer of defence, not the only one.

For courts and the police: build capacity.

1. Set up specialised cyber cells with trained officers and a single national reporting channel for deepfake complaints, available in regional languages.
2. Develop standard protocols for authenticating digital audio and video, and empanel accredited forensic laboratories whose reports courts can rely on.
3. Encourage courts to issue dynamic injunctions that cover mirror sites and re-uploads, while insisting on proportionality.

For schools, workplaces and families: prevention and awareness.

1. Add media literacy and digital consent to school and college curricula, since many offenders and victims are young.
2. Encourage companies to adopt verification steps, such as call-backs and second approvals for payments, to blunt voice and video fraud.
3. Run public campaigns that tell people exactly what to do if they are targeted: save evidence, report to the platform's grievance officer, file a complaint on the national cybercrime portal, and seek help early.

For international cooperation.

India should work with other countries on shared standards for provenance, faster cross-border evidence requests and common definitions. Because deepfakes ignore borders, enforcement that stops at the border will always be partial.

8. Conclusion

Deepfakes force the law to answer an old question in a new setting: who controls a person's identity, and what do we owe each other when seeing and hearing can no longer be trusted? The technology is neither purely good nor purely bad. Its harms, however, are concrete and fall

hardest on those least able to defend themselves: women and girls targeted with intimate fakes, families deceived by cloned voices, and voters misled at critical moments.

India has moved more quickly than many expected. The 2026 amendment to the IT Rules gives the country a definition of synthetic content, labelling duties and some of the shortest takedown deadlines anywhere, and the High Courts have shown that personality rights can be stretched to meet the AI era. Yet the framework still leans heavily on subordinate rules and interim court orders. It lacks a dedicated offence for creating harmful deepfakes, a direct civil remedy for ordinary victims, and clear statutory protection for satire and dissent.

The international picture suggests that no single tool is enough. The strongest responses combine criminal law for the worst conduct, fast and fair platform duties, honest transparency measures, and a genuine right for individuals to control their likeness. They also invest in the less glamorous work of training police, equipping courts and educating the public.

The central lesson is that law must protect trust without sacrificing freedom. A system that is too weak leaves victims exposed; one that is too aggressive turns platforms into censors. The task for lawmakers, judges and technologists is to find the narrow path between the two, and to keep adjusting it as the technology changes. For the student of law, that is what makes this subject so compelling: it is a live test of whether legal institutions can adapt at the speed of innovation without losing sight of the human beings they exist to serve.

References

Below is your complete bibliography reformatted in a consistent Indian Law Institute (ILI) citation style, with separate headings for statutes, rules and treaties, judicial decisions, books, journal articles, research reports and online sources.

I have standardised author names, titles, italics, volume numbers, page references, publication details, DOI references and web citations. I have also corrected the numbering and separated the ILO report, which was previously merged with Reference 19.

BIBLIOGRAPHY

I. Statutes, Rules and International Legal Instruments

1. The Information Technology Act, 2000 (Act 21 of 2000), §§ 66C, 66D, 66E, 67, 67A, 67B, 69A and 79 (India).

2. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), §§ 77, 79, 318, 319, 336, 351 and 356 (India).

3. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023) (India).

4. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023) (India).

5. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended (India).

6. TAKE IT DOWN Act, Pub. L. No. 119-12 (2025) (United States).

7. 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), art. 50, 2024 O.J. (L).

8. 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).

9. Data (Use and Access) Act 2025 (United Kingdom).

10. Online Safety Act 2023 (United Kingdom).

II. Judicial Decisions

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

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

13. Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi High Court, 20 September 2023).

14. Raj Shamani v. John Doe & Ors., (Delhi High Court, 2025).

15. Ravi Shankar v. John Doe(s)/Ashok Kumar(s) & Ors., (Delhi High Court, 2025).

III. Books, Journal Articles and Research Publications

16. Ian Goodfellow et al., “Generative Adversarial Nets” in Advances in Neural Information Processing Systems 27, 2672–2680 (2014).

17. Sree Parvathavarthini S.K. and Santosh Kumar Tiwari, “Deepfake Technology: Legal Challenges and Regulatory Responses” 6(9) Indian Journal of Legal Review 774–787 (2026), ISSN: 2583-2344.

18. Radha Ranjan, Cyber Law Essential: Law, Technology & Practice (Integrity Education India, New Delhi, 2026), ISBN: 978-93-47508-68-4.

19. Robert Chesney and Danielle Keats Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security” 107 California Law Review 1753–1820 (2019).

20. Amaresh Patel, Aarti Patel, Deependra Nath Pathak, Karunesh Shukla, Arpita Mishra and Radha Ranjan, “Artificial Intelligence Regulation and Governance: A Comparative Doctrinal Analysis of Emerging Legal Frameworks” (2026), SSRN, DOI: 10.2139/ssrn.7116699.

21. International Labour Organization, World Employment and Social Outlook 2021: The Role of Digital Labour Platforms in Transforming the World of Work (International Labour Office, Geneva, 2021).

22. Radha Ranjan, “Evolution of the Doctrine of Proportionality: Assessing its Scope and Ambit in Relation to the Right to Privacy in India” 10(1) Indian Journal of Law and Human Behavior 31–38 (2024), ISSN: 2454-7107, e-ISSN: 2455-4189.

23. Radha Ranjan, Jayini Bhaumik and Amaresh Patel, “Regulating Artificial Intelligence in Legal Practice: An Accountability Framework” in Blockchain and AI in Business: Applications, Research and Insights 131–140 (Gyanavi Publishers & Distributors, 2024).

24. Deeptrace, The State of Deepfakes: Landscape, Threats, and Impact (2019).

25. Radha Ranjan, “Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches” in Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches 217–263 (IGI Global Scientific Publishing, 2026), DOI: 10.4018/979-8-3373-5992-2.ch007.

IV. Online Articles, News Reports and Web Commentary

26. BRB Legal, “IT Rules 2026: AI Content Labels, Deepfakes and Takedowns” (2 November 2026), available at: BRB Legal (last visited Nov. 6, 2026).

27. Bar & Bench, “Delhi High Court Protects Sri Sri Ravi Shankar's Personality Rights Against Circulation of Deepfakes, AI Videos”, available at: Bar & Bench (last visited Nov. 6, 2026).

28. Storyboard18, “Delhi HC Orders Takedown of Ajay Devgn Deepfakes, Upholds Personality Rights” (28 November 2025), available at: Storyboard18 (last visited Nov. 6, 2026).

29. Storyboard18, “Kajol, Aishwarya Rai, and Other Celebrities Who Went to Court to Protect Their Personality Rights”, available at: Storyboard18 (last visited Nov. 6, 2026).

30. Guru Legal, “Personality Rights in the Digital Age: Raj Shamani and AI Deepfakes”, available at: Guru Legal (last visited Nov. 6, 2026).

31. The 420.in, “Deepfake Scam: How to Spot AI-Generated Video and Images Used in Fraud”, available at: The 420.in (last visited Nov. 6, 2026).

32. Orrick, “TAKE IT DOWN Act Becomes Law” (May 2025), available at: Orrick (last visited Nov. 6, 2026).

33. GDPRLocal, “EU AI Act Article 50 Transparency Rules for Businesses”, available at: GDPRLocal (last visited Nov. 6, 2026).

34. Why AI Man, “EU AI Act Transparency Obligations Now In Force” (August 2026), available at: Why AI Man (last visited Nov. 6, 2026).

35. BABL AI, “UK Government Introduces Crackdown on 'Deepfakes' Creation”, available at: BABL AI (last visited Nov. 6, 2026).

36. Bird & Bird, “New AI Content Labelling Rules in China: What Are They and How Do They Compare to the EU AI Act?” (2025), available at: Bird & Bird (last visited Nov. 6, 2026).

37. The Korea Herald, “Cabinet Passes New Bill to Criminalize Even Possession of Deepfake Porn” (10 October 2024), available at: The Korea Herald (last visited Nov. 6, 2026).

38. TimesLIVE, “South Korea to Criminalise Watching or Possessing Sexually Explicit Deepfakes” (26 September 2024), available at: TimesLIVE (last visited Nov. 6, 2026).

39. Euronews, “Denmark Introduces Bill to Protect People's Faces and Voices from Deepfakes” (8 October 2026), available at: Euronews (last visited Nov. 6, 2026).