INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DEEPFAKE TECHNOLOGY AND CRIMINAL LAW IN INDIA: ADDRESSING RISKS TO DIGITAL IDENTITY, PRIVACY, AND REPUTATION

AUTHORED BY - MADHUMITA CHOUDHURY

Abstract

Deepfake technology has come a long way, and now people can make audio, images, and videos that look and sound real. The main reason for this progress is that artificial intelligence is getting better all the time. This technology can be useful for new digital ideas, education, and entertainment. But if you use it wrong, it can cause big legal and moral problems. Deepfakes are being used more and more to change digital content, which is a big threat to privacy, reputation, and digital identity. Because of this, people are more vulnerable online, especially with the rise of fake news, identity theft, and deepfake porn that isn't consensual. This study examines deepfake technology's impact on Indian criminal law. The Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, are examined for their effectiveness in addressing AI-generated synthetic media offences. It highlights legal issues like the lack of deepfake legislation, detection and investigation challenges, and online platform responsibilities. Based on a comparative analysis of relevant scenarios, the paper stresses the need for a comprehensive regulatory framework to address growing technological concerns. Further, examines constitutional development and judicial recognition of privacy and digital rights.

Keywords: Deepfake Technology, Digital identity, Privacy, Cybercrime, Criminal law.

Introduction

The development of artificial intelligence, especially in machine learning and deep learning, has made it easier to make fake media, which are often called "deepfakes." The word "deepfake" combines "deep learning" and "fake" to mean changing real pictures.[1] Deepfake technology has become a major focus of legal and ethical scrutiny because it is becoming easier

[1] Sharma, Isha, and Biranchi Naryan P. Panda. "Deepfake Technology in India and World: Foreboding and Forbidding." *OSF Preprints (OSF Preprints)*, 2025, https://osf.io/7w8c2.

ISSN: 2582-6433

to get and has more advanced features. This is because it blurs the line between real and fake digital content.[2] Artificial sounds, films, and images can be created with deepfake technology. Women often face harassment, threats, or revenge porn, which can harm their mental health and reputations. Fake propaganda also manipulates public opinion to undermine democracy and disseminate lies. These abuses show how easy it is to use deepfakes and how well they can hide the truth. This increases the likelihood of identity theft or scams targeting individuals. This poses a significant threat to trust, privacy, and safety. For instance, the creation of sexual content without consent is a serious issue. This enables identity theft, spreading fake information, and unauthorised creations easier.[3] India has no deepfake legislation despite AI-generated fake news and identity theft. Conventional cybercrime, defamation, and data protection laws ignore synthetic media. Independent AI operations may not be prosecuted or identified for dark web fraud under current legislation. Hence the Information Technology Act and Indian Penal Code should be amended to handle its particular issues. Deepfakes pose complicated challenges to digital identity, privacy, and reputation. India's criminal justice system's capacity to address technological challenges and deficiencies is also assessed. The main moral issue between free expression and the necessity to know the truth and manage this technology to avoid harm is also examined. This paper discussed Indian law that fails to criminalise deepfake crimes like stealing someone's identity or hurting their reputation. The law would fill the gap and protect individuals from the risks. Furthermore, the study will approach controlling deepfakes throughout the world and then apply those ideas to make Indian legislation stronger.

Concept and Evolution of Deepfake Technology

Deepfake technology employs adversarial networks, which are generative or automated encoders, to edit or make up audio and video data. This makes lifelike simulations that are hard to discern apart from real media. This extensive manipulation makes it hard for the law and morality to tell the difference between real and fake digital information and need to learn about the technology that makes deepfakes feasible since they can generate fake material that seems quite authentic.[4] For instance, deepfakes have been used to make explicit content without the

[2] Kaur, Shraileen, and Vivek Kumar. "Consumer Protection and Deep Fakes - Assessing the Rights and Remedies for Victims in India." 12 *International Journal for Research in Applied Science and Engineering Technology*, 1032, (Apr. 2024) , https://doi.org/10.22214/ijraset.2024.59830.
[3] Kashyap, Sommya. "The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology." *22 A Journal of Law Technology & Society*, 162 (Dec. 2025) https://doi.org/10.2218/scrip.22.2.2025.12004.
[4] Sharma, Isha, and Biranchi Naryan P. Panda. "Deepfake Technology in India and World: Foreboding and Forbidding." *OSF Preprints (OSF Preprints)*, (July 2025), https://osf.io/7w8c2.

ISSN: 2582-6433

consent of Indian women, which has caused a lot of damage to their reputations and mental pain for the victims. In addition to sexual material, deepfake technology has been used in India to commit financial fraud using voice cloning, where criminals copy people's voices to approve fake transactions or pretend to be officials to get important information. This advanced manipulation makes it hard to tell what's real and what's phoney, which makes it hard for legal and ethical institutions to keep an eye on digital information. Deepfakes may make fake material that seems quite real, therefore it's crucial to know how they work. and the chance that it may be used wrong in different situations. It might be hard to see these changes.[5]

Deepfake technology is often used for bad things, but it may also be useful in entertainment, education, and the arts. technology is used in Hollywood to make actors seem younger or bring back stars who have died, which shows how useful technology is for making movies. Deepfakes also improve education by making it possible to have lectures from famous people or interactive training modules. For example, researchers have used deepfakes to make AI Human Professor Models that act as virtual teachers giving interesting lessons for the Fourth Industrial Revolution. Deepfakes also create fake datasets for training diagnostic AI systems and realistic patient models for surgical rehearsals in medicine. This makes medical training and research better.[6] But others use deepfakes illegally to generate pornographic content without authorisation, commit fraud, and spread misleading information that alters people's opinions and harms democracy. Some of the negative things that these unlawful apps do are stealing people's identities, harassing them, committing intricate financial scams, and messing with elections.[7] These bad deepfakes spread swiftly, hurt people, and are continually changing, which makes them a big threat to both people and the stability of society.[8]

Several nations have indicated that crimes that use deepfake technology have grown a lot in the previous few years. Some of these people are making porn that seems real without permission, stealing money, spreading false information about politics, stealing someone's identity, and damaging their reputation. People have used deepfake movies to pretend to be

[5] *Supra* note 2.
[6] Chun, Yang-Ha, and Soo-Yeon Yoon. "Creating an AI Human Professor Model to Implement a New Educational Paradigm of the 4th Industrial Revolution." 19 *Tehnički Glasnik*, 587 (Sept. 2025), https://doi.org/10.31803/tg-20250326033909.
[7] A Miotti and Akash R. Wasil, "Combatting deepfakes: Policies to address national security threats and rights violations" *arXiv (Cornell University)* (2024). arXiv:2402.09581
[8] Krishna, Dhruva, Deepfakes, Online Platforms, And A Novel Proposal for Transparency, Collaboration, And Education (April 19, 2021). Available at SSRN: https://ssrn.com/abstract=5080139 or http://dx.doi.org/10.2139/ssrn.5080139

ISSN: 2582-6433

renowned people and business leaders in order to spread false information or commit fraud. This kind of fake news travels so swiftly on social media that it puts people and companies at a higher risk of damage. The United States, China, and the United Kingdom are some of the countries that have begun to pass laws to stop the exploitation of deepfake technology because they see these problems getting worse. But several countries, including India, still apply their current cybercrime laws instead of laws that solely deal with deepfake offences. As deepfake crimes happen more and more over the world, it becomes evident how important it is to have strong courts that can deal with the legal and technological problems that AI-generated fake media causes.[9]

Risks of Deepfake Technology

Deepfake technology in India makes things like financial fraud, rigging elections, and violence against women and children worse since AI is being utilised more swiftly and regulations aren't being developed fast enough. Cases have gone up by 90% recently, with 93% of them impacting women through non-consensual porn. BEC fraud is also a problem for businesses, and false information is a threat to democracy.[10] Deepfakes aren't simply deceiving cameras; they're also hurting women the most by converting images into a new sort of weapon. Recent research from the creative intelligence platform Pi-labs has shown that over 93% of deepfake victims are women. In the last several years, deepfake material aimed at women has grown by nine times. In India, more than a third of women who are harassed online don't do anything about it, and many women cut back on their internet activity after being abused. Almost a thirty three percent of women still don't know about laws that protect them.[11] Deepfakes, which employ powerful AI, let people change photographs, videos, and sounds without asking. This violates the right to privacy as established in *Justice K.S. Puttaswamy* v. *Union of India*.[12] This is an abuse of technology that goes beyond hacking. It also includes identity theft, which is when someone takes someone else's photograph for illicit purposes. Recent case of Delhi High Court grants an injunction against AI generated pornographic content, ordering takedown, de-indexing, and disclosure of perpetrators, thereby recognising such material as a **serious**

[9] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 107 *California Law Review* 1753 (2019).
[10] Editorial, "65% of Indian organisations hit by deepfake attacks: Report" *GCC WORLD.COM*, Mar 9, 2026. *Available at*: https://gcc.economictimes.indiatimes.com/news/deepfake-attacks-surge-amid-ai-adoption-in-indian-organizations/129321078. (Mar 28, 2026).
[11] *Editorial, "Deepfakes target women in 93 per cent of cases, report finds" IndianTelevision.Com, march 10, 2026. Available at: https://indiantelevision.com/mam/deepfakes-target-women-in-93-per-cent-of-cases-report-finds/. (Mar 28, 2026).*
[12] (2017) 10 SCC 1.

ISSN: 2582-6433

violation of privacy and dignity.[13] In a 2025 instance with a woman victim, the same court granted temporary relief against the spread of non-consensual explicit deepfake content, saying that this kind of spread is a serious violation of basic rights, such as privacy and reputation.[14] The number of AI-created child sexual assault videos and pictures was up by 1,325% from 2023 to 2024. According to UNICEF, this affects 1.2 million kids every year. "Nudification" programs turn pictures into false nudes, which makes it easier for people to take advantage of others and harder for the authorities to execute their jobs.[15] It's harder to do investigations since it's hard to determine if deepfake information is real and where it comes from. It's also hard to the authorities to figure out who made it and arrest them. People are using deepfakes more and more as weapons to spread false political information, modify the stories told during elections, or start violence. Fake recordings of politicians making contentious comments have appeared in a number of countries, putting the peace of society and the validity of democracy at risk. Deepfake crimes are very serious for your mental health. A lot of people who have been the victims of deepfake pornography, identity theft, and defamation feel anxious, sad, and emotionally hurt. False information may make people feel powerless, ashamed, and alone since it's hard to verify, especially when it looks real. Being on the internet makes victims feel bad about themselves and hurts their reputations.[16]

Legal Framework Against Deepfake Technology

Although deepfakes are not yet specifically govern by law in India, these damages are addressed through a combination of criminal law, cyber law statutes, and constitutional provisions. There aren't clear restrictions in India for deepfake technology. It doesn't just employ cyber laws, criminal laws, and constitutional difficulties. Article 21 of the Constitution, which protects identity, privacy, and dignity, lies at the core of it.[17] The Supreme Court's acknowledgement of personal liberty and informational privacy establishes a strong constitutional foundation for challenging the unlawful production and distribution of deepfake content. This decision sets a baseline, but it doesn't say how to deal with new technologies like deepfakes, thus legislations are required.[18]

[13] *X v. John Doe* CS(OS) 33/2026.
[14] *Kamya Buch v. JIX5A & Ors.* **2025 SCC OnLine Del 6428.**
[15] **United Nation, "Deepfake abuse is abuse,' UNICEF warns" UN NEWS, 4 Feb, 2026. *Available at:* https://news.un.org/en/story/2026/02/1166886**
[16] Jaya Sharma, "DEEPFAKE CRIMES: EMERGING THREATS AND LEGAL CHALLENGES IN THE DIGITAL ERA" 7 Indian Journal of Law and Legal Research 1392 (2025).
[17] *K.S. Puttaswamy* v *Union of India* (2017) 10 SCC 1.
[18] ***Akshaya R,* "An Analysis on Artificial Intelligence and Data Privacy in India" 7 *Indian Journal of Law and Legal Research* 4918 (2025).**

ISSN: 2582-6433

The major law in India that deals with cybercrimes is the Information Technology Act of 2000. It builds on this. Sections 66C and 66D deals with stealing someone's identity and pretending to be them. Sections 67, 67A, and 67B make it unlawful to have or share sexually graphic or obscene information, especially on child sexual abuse. These rules are very vital for banning deepfake porn that targets women and children without their permission. Experts claim that the Act is out of date, though, because it doesn't make it apparent which manipulations are made by AI. This makes it impossible to interpret and execute.[19] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[20] also require intermediaries to do their due diligence by removing illegal information and setting up ways for people to complain. These rules offer some protection for procedures, but they aren't very successful because people don't always follow them right away and deepfake stuff spreads quickly. Research shows that delayed takedown methods can make things worse, especially in situations of image-based sexual assault, when victims keep suffering reputational and psychological harm long after they report it.

The Bharatiya Nyaya Sanhita, 2023 criminal law, and cyber laws provides remedies for offences such defamation, cheating by impersonation, criminal intimidation, and outraging women's modesty.[21] India is employing these laws more and more to stop blackmail, sextortion, and the distribution of bogus pornographic information, especially against women and young people on social media. More and more crooks are using AI-generated movies or voice clones to collect money or make people do things, usually by threatening to expose bogus personal information. In these situations, the IT Act's provisions are used along with laws against extortion, criminal intimidation, and insulting modesty. Notwithstanding their relevance, the application of the Bharatiya Nyaya Sanhita, 2023 framework in deepfake scenarios exposes considerable doctrinal and practical constraints. First, classic crimes like defamation and outraging modesty were thought of before the digital age, and they don't fully convey the volume, speed, and permanence of the damage produced by AI-generated information. Once a deepfake video is posted, it may be copied and shared on many platforms in just a few minutes. This makes the damage immediate and permanent, which current criminal laws do not completely cover. Second, the Bharatiya Sakshya Adhiniyam, 2023, makes it hard to prove the truth or falsehood of digital communication. Deepfakes make it hard to tell the difference

[19] Dr. Suresh Kumar, "Freedom of expression in social media" 12 International Journal of Law 86 (2026).
[20] Ministry of Electronics and IT, *IT Rules, 2021*.
[21] The Bharatiya Nyaya Sanhita, 2023, s. 356, 319, 351, 74.

ISSN: 2582-6433

between genuine and fake evidence, which makes it harder to verify forensic evidence and raises the chance of someone being wrongly accused or found not guilty.[22]

The Digital Personal Data Protection Act, 2023[23] also sets up a system for processing personal data based on consent. This indirectly deals with problems with the unlawful use of personal information. This is an important step toward better data protection, but it doesn't do enough to control how people may change publicly available photos or synthetic media. This is a major issue when it comes to dealing with deepfake technology.[24]

Judicial Approaches

There isn't a particular legislation in India that deals with the recent harm caused by deepfake technology, but judicial interpretation has been highly essential in changing existing legal ideas to cope with them. The Supreme Court of India expanded the scope of Article 21 by acknowledging the right to privacy as a fundamental right.[25] This includes the right to control one's own identity and choose what information to share. Particularly when an individual's image is altered without their consent, this perspective provides a strong constitutional foundation for addressing the issues of deepfakes. The Court in the *Shreya Singhal case*,[26] for example, clarified that online expression that causes defamation, harassment, or incitement is still subject to reasonable restrictions, thereby facilitating the regulation of detrimental deepfake content under existing criminal law, while also protecting freedom of speech.

The right to privacy is frequently at odds with the freedom of expression, which is not unrestricted under Article 19(1)(a) of the Indian Constitution. The Court clarified in the *Indian Express Newspapers (Bombay) (P) Ltd*[27] case, that the right to freedom of speech must be balanced with the right of an individual to maintain their dignity and reputation. While judicial interpretations of Article 19(1)(a) in cases such as *S. Khushboo*[28] and *Ashutosh Dubey*[29] have broadened the purview of freedom of speech in relation to parodies and satire, the freedom is

[22] *Supra* note 16.
[23] The Digital Personal Data Protection Act, 2023 (Act. 22 of 2023).
[24] Graham Greenleaf, 'Global Data Privacy Laws 2023' 169 *Privacy Laws & Business International Report* 10 (2023).
[25] *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
[26] *Shreya Singhal v. Union of India* (2015) 5 SCC 1.
[27] *Indian Express Newspapers (Bombay) (P) Ltd. v. Union of India (***1986) AIR 515, 1985 SCR (2) 287, 1985 SCC (1) 641).**
[28] *S. Khushboo* v. *Kanniammal*, (2010) 5 SCC 600: (2010) 2 SCC (Cri) 1299.
[29] *Ashutosh Dubey* v. *Netflix Inc*, (2010) 5 SCC 600; 2020 SCC OnLine Del 625.

ISSN: 2582-6433

also restricted in its capacity to breach the boundaries of defamation or obscenity. As a result, this category may include deepfakes that satirise or parody public figures; however, the claimant must differentiate between constitutionally protected satirical content and harmful, deceitful, or malevolent representations.[30]

In addition, Indian courts have begun to acknowledge the significance of digital evidence and its authenticity, as evidenced by the *Anvar P.V.* v. *P.K. Basheer case*[31], which mandated stringent adherence to evidentiary requirements for electronic records. *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal*,[32] reaffirmed this principle, emphasizing the importance of certification under evidentiary law to guarantee reliability. Although these rulings expose the limitations of existing standards in detecting AI-generated falsification, they also underscore the judiciary's commitment to preserving evidentiary integrity and averting manipulation in the context of deepfakes.

High Courts in India have also made a substantial contribution by acknowledging reputational interests and personality rights in the digital domain. The Delhi High Court issued a comprehensive injunction to safeguard the actor's name, image, and voice from unauthorized commercial exploitation, thereby confirming the enforceability of personality rights against digital misuse.[33] In similar way, the Bombay High Court and related proceedings involving actor Akshay Kumar issued urgent suppression orders against AI-generated videos, asserting that such deepfakes infringe upon the rights of individuals, their dignity, and public safety, particularly when the fabricated content has the potential to incite social unrest.[34]

This approach has been expanded in recent deepfake-related cases, where courts have granted John Doe injunctions and suppression orders to prevent the circulation of manipulated content, acknowledging the irreparable damage to identity, reputation, and dignity. Moreover, courts have recognized the gendered aspect of online abuse, particularly in instances involving non-

[30] Yash Bajpai, Me, Myself and AI: Chasing Deepfakes Across Borders Without Losing Your Rights, *SSC Online Time*, Nov 8, 2025, available at: https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/ ((Mar 30, 2026).
[31] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.
[32] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
[33] *Amitabh Bachchan v. Rajat Nagi* 2022 SCC OnLine Del 4116, sec also Delhi High Court grants ex-parte ad-interim injunction to Amitabh Bachchan protecting his publicity rights, *SSC Online.Com.* Nov 28, 2022. *available at:* https://www.scconline.com/blog/post/2022/11/28/delhi-high-court-grants-ex-parte-ad-interim-injunction-to-amitabh-bachchan-protecting-his-publicity-rights/ (Mar 30, 2026).
[34] *Akshay Hari Om Bhatia v. John Doe*, Bombay High Court, 2025.

ISSN: 2582-6433

consensual intimate pictures. The court in *Subhranshu Rout* v. *State of Odisha* case,[35] emphasized the severe psychological and social consequences of such actions, regard them as grave violations of privacy and dignity. Such reasoning is directly pertinent to cases of deepfake pornography, in which the harm does not limit itself to obscenity but also encompasses digital sexual exploitation and identity violation.

Conclusion

AI enhances efficiency and decision-making but raises concerns about mass surveillance, data abuse, and discrimination. While the DPDP Act, 2023, and IT Act, 2000, guarantee privacy, they do not address AI privacy issues. India should emphasize AI regulation, user consent, responsibility for AI data breaches, and open AI-based decision-making. Technical progress and privacy rights must be balanced in India's AI future. AI without a robust legal framework might cause data misuse, cybersecurity risks, and autonomy loss. The government, courts, and industry partners must collaborate on AI-specific privacy and innovation laws. India should adopt these legal and policy steps to solve AI-driven data privacy challenges.

References

- Sharma, Isha, and Biranchi Naryan P. Panda. "Deepfake Technology in India and World: Foreboding and Forbidding." *OSF Preprints (OSF Preprints)*, 2025, https://osf.io/7w8c2.
- Kaur, Shraileen, and Vivek Kumar. "Consumer Protection and Deep Fakes - Assessing the Rights and Remedies for Victims in India." 12 *International Journal for Research in Applied Science and Engineering Technology*, 1032, (Apr. 2024) , https://doi.org/10.22214/ijraset.2024.59830.
- Kashyap, Sommya. "The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology." *22 A Journal of Law Technology & Society*, 162 (Dec. 2025) https://doi.org/10.2218/scrip.22.2.2025.12004.
- Sharma, Isha, and Biranchi Naryan P. Panda. "Deepfake Technology in India and World: Foreboding and Forbidding." *OSF Preprints (OSF Preprints)*, (July 2025), https://osf.io/7w8c2.

[35] *Subhranshu Rout v. State of Odisha* 2020 SCC OnLine Ori 878.

ISSN: 2582-6433

- Chun, Yang-Ha, and Soo-Yeon Yoon. "Creating an AI Human Professor Model to Implement a New Educational Paradigm of the 4th Industrial Revolution." 19 *Tehnički Glasnik*, 587 (Sept. 2025), https://doi.org/10.31803/tg-20250326033909.
- A Miotti and Akash R. Wasil, "Combatting deepfakes: Policies to address national security threats and rights violations" *arXiv (Cornell University)* (2024). arXiv:2402.09581
- Krishna, Dhruva, Deepfakes, Online Platforms, And A Novel Proposal for Transparency, Collaboration, And Education (April 19, 2021). Available at SSRN: https://ssrn.com/abstract=5080139 or http://dx.doi.org/10.2139/ssrn.5080139
- Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 107 *California Law Review* 1753 (2019).
- Editorial, "65% of Indian organisations hit by deepfake attacks: Report" *GCC WORLD.COM*, Mar 9, 2026. *Available at*: https://gcc.economictimes.indiatimes.com/news/deepfake-attacks-surge-amid-ai-adoption-in-indian-organizations/129321078. (Mar 28, 2026).
- *Editorial, "Deepfakes target women in 93 per cent of cases, report finds" IndianTelevision.Com, march 10, 2026. Available at: https://indiantelevision.com/mam/deepfakes-target-women-in-93-per-cent-of-cases-report-finds/. (Mar 28, 2026).*
- *X v. John Doe* CS(OS) 33/2026.
- *Kamya Buch v. JIX5A & Ors.* **2025 SCC OnLine Del 6428.**
- **United Nation, "Deepfake abuse is abuse,' UNICEF warns" UN NEWS, 4 Feb, 2026. *Available at:* https://news.un.org/en/story/2026/02/1166886**
- Jaya Sharma, "DEEPFAKE CRIMES: EMERGING THREATS AND LEGAL CHALLENGES IN THE DIGITAL ERA" 7 Indian Journal of Law and Legal Research 1392 (2025).
- *K.S. Puttaswamy* v *Union of India* (2017) 10 SCC 1.
- ***Akshaya R,* "An Analysis on Artificial Intelligence and Data Privacy in India" 7 *Indian Journal of Law and Legal Research* 4918 (2025).**
- Dr. Suresh Kumar, "Freedom of expression in social media" 12 International Journal of Law 86 (2026).
- Ministry of Electronics and IT, *IT Rules, 2021.*
- The Bharatiya Nyaya Sanhita, 2023, s. 356, 319, 351, 74.

ISSN: 2582-6433

- The Digital Personal Data Protection Act, 2023 (Act. 22 of 2023).
- Graham Greenleaf, 'Global Data Privacy Laws 2023' 169 *Privacy Laws & Business International Report* 10 (2023).
- *Shreya Singhal v. Union of India* (2015) 5 SCC 1.
- *Indian Express Newspapers (Bombay) (P) Ltd. v. Union of India (***1986) AIR 515, 1985 SCR (2) 287, 1985 SCC (1) 641).**
- *S. Khushboo* v. *Kanniammal*, (2010) 5 SCC 600: (2010) 2 SCC (Cri) 1299.
- *Ashutosh Dubey* v. *Netflix Inc*, (2010) 5 SCC 600; 2020 SCC OnLine Del 625.
- Yash Bajpai, Me, Myself and AI: Chasing Deepfakes Across Borders Without Losing Your Rights, *SSC Online Time*, Nov 8, 2025, available at: https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/ ((Mar 30, 2026).
- *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
- *Amitabh Bachchan v. Rajat Nagi* 2022 SCC OnLine Del 4116, sec also Delhi High Court grants ex-parte ad-interim injunction to Amitabh Bachchan protecting his publicity rights, *SSC Online.Com.* Nov 28, 2022. *available at:* https://www.scconline.com/blog/post/2022/11/28/delhi-high-court-grants-ex-parte-ad-interim-injunction-to-amitabh-bachchan-protecting-his-publicity-rights/ (Mar 30, 2026).
- *Akshay Hari Om Bhatia v. John Doe*, Bombay High Court, 2025.
- *Subhranshu Rout v. State of Odisha* 2020 SCC OnLine Ori 878.