Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

Violation of Human Rights vis-a-vis Misuse of Artificial Intelligence through Deepfake: Challenges and Regulatory Framework

Dr Seema Saini
Ph.D. Scholar, Department of Law,
Gurugram University

Submission date 12.04.2026 | Acceptance date: 25.04.2026 | Publication: 29.05.2026

ABSTRACT

The rise of Artificial Intelligence (AI) in public spaces threatens privacy concerns. It is witnessed that AI is being misused on social media by creating fake photos and videos by using pictures of an individual used on social media. Individuals are threatened by privacy breach by misusing social media content. There are many other challenges like privacy surveillance, freedom of speech and expression, algorithmic basis & discrimination, misinformation and deep fakes. This paper covers the aspect of human rights violations due to deepfakes. Deepfake pictures are being created, edited, and misused with body changes, voice changes, or faces changed with someone else. This disturbs the victim mentally and creates tension. The objective of this paper is to study real-life examples of deep fakes, which show their human rights violations by conducting quantitative research. During this research, real life case-studies from newspapers, articles showing the veracity and grievances of the victim are conducted. The research question for this doctrinal research is to find out whether deepfake pictures violate the right to privacy and whether the right to privacy is a human right of an individual. It is also to explore how an individual can be affected by an unknown person. At the end, an analytical study of the regulatory framework is done, to show the available and required laws for dealing with deepfakes.

Keywords: Deepfake, Cybercrime, Cybersecurity, Celebrity, Misinformation, Human rights, fundamental rights

I. INTRODUCTION

The rapid growth of using artificial intelligence is increasing not only as a helping tool but also for amusement. AI does not think as human, but it helps and assists humans by giving reasoning and creativity through a mechanical process. Stanford AI Index Report 2024 mentions that now companies are integrating AI into daily workflows and this has increased their productivity by 30 %.[1] In education and research, students also take help from AI. The misuse of the same is also increasing, and it is affecting everywhere, be it research, education, medicine, mass media, social media, etc. This paper is confined to the study of misuses of AI in social media. With the help of technology fake images are created where it would be difficult to distinguish from the real one.

[1] Jeet Padhya, "AI is a Tool, Not a Replacement: How Artificial Intelligence Amplifies Human Capability", *available at* https://medium.com/@jeetpadhya35/ai-is-a-tool-not-a-replacement-how-artificial-intelligence-amplifies-human-capability-7a798ba864d2 (last visited on April 6, 2026).

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

We post a picture on social media, the evil minds can create a synthetic image with the help of AI. Deepfake refers to hyper-realistic media that is synthetically generated by AI.[2] "As its name implies, the term "deepfake" is derived from the combination of "deep" [referring to *deep learning* (DL)] and "fake." It is normally used to refer to the manipulation of existing media (image, video, and/or audio) or the generation of new (synthetic) media using DL-based approaches."[3] In this activity pictures are created using different face-changing tools, photo editing tools, and video editing tools. The purpose of creating fake pictures are often used to spread misinformation and create fraudulent content just to damage reputations. This act is done with a guilty mind, hence same attracts criminal liability and civil liability for harming the reputation of the concerned person. Indeed, this is mental harassment to such persons whose fake photos are floating and being trolled badly on social media. In the discussion of this paper, all the important laws and legal provisions are being discussed. Most significant and viral case studies that become more controversial are also discussed. Mostly, these activities happen with celebrities or high-profile people.

As an issue, this deep fake activity is a challenge to human privacy and there are high chances of privacy breach. Right to privacy is our fundamental right and some fundamental rights are human rights also. This deep fake technology is used for the entertainment purpose but they are widely used for malicious purpose also where non-consensual intimate imagery and political misinformation is created. No doubt deepfakes create high risks to cybersecurity and blur the line between real and manipulated.

II. CASE STUDY

A rapidly growing market from AI-powered fake endorsements is revealed by the research done by McAfee labs[4] in 2025, showing the deepfake deception list, where celebrities are listed and influencers whose likeness is most frequently used by con artists. At the very top, Tylor swift, Sydney Sweeney, Jenna Ortega, Scarlett Johansson, Emma Watson, Brad Pitt, and many more are exploited worldwide by the AI synthetic audio and video scams. This research unveiled its first-ever influencer deepfake deception list, with Pokimane, who is a top gamer and streamer, being targeted by this deepfake activity. Its shows that the scammers are now targeting social media platforms with the same ferocity as Hollywood.

Not in only Hollywood but also Bollywood and top politicians are facing these deepfake concerns. McAfee research also listed the Indian actors and actresses who are victimized by

[2] Dr. A. Shaji George, & A. S. Hovan George, "Deepfakes: The Evolution of Hyper realistic Media Manipulation", *1*(2), *Partners Universal Innovative Research Publication*, 58–74. (2023) https://doi.org/10.5281/zenodo.10148558

[3] Altuncu E, Franqueira VNL, Li S. "Deepfake: definitions, performance metrics and standards, datasets, and a meta-review" *Front Big Data.* 2024 Sep 4;7:1400024. doi: 10.3389/fdata.2024.1400024. PMID: 39296632; PMCID: PMC11408348.

[4] McAfee is a prominent cybersecurity company that provides comprehensive, award-winning software. It is designed to defend personal computers, tablets and smartphones against viruses, malware, ransomware and phishing attacks. It protects machines by providing real-time scanning, identity monitoring and a secure VPN to ensure safe browsing

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

deepfake audio-video pictures. Deepfake deception list provided by McAfee research[5] mentions that at the top of the list is Shah Rukh Khan, Alia Bhat, Elon Musk, Priyanka Chopra Jonas, who are under deepfakes issues. "In the politician hon'ble PM Narendra Modi and Finance Minister Smt. Nirmala Sitaraman has also faced this issue of deepfakes. In the McAfee report, it is given that approx 90% are exposed to fake AI-generated celebrity endorsement in India, with victims losing an average of Rs 34,500 daily. Its Deepfake deception list shows how cyber-criminals used the names and likenesses of celebrities to trick people into scams."[6]

"Technology can now effortlessly mimic the voices, faces, and mannerisms of people we admire."[7] McAfee research highlighted that mostly youngsters are facing this risk. About 62 % of people aged between 35 to 44 and 60% of 25 to 34-years-old youngsters fell into prey of online fraud done through synthetic video ads. Some of Bollywood's biggest stars, including Aishwarya Rai Bachan and her husband, with Director Karan Johar, have filed the case before Delhi High Court to safeguard their personality rights against the exploitation of deepfakes created by AI. It is always produced for profit, but occasionally it contains offensive or sexually explicit content. In the case of Aishwarya Bachan Delhi High Court passed an order in favour of victim and ordered the removal of infringing content and barred the online platform from using illegally using her name or images for profit.[8]

In 2024, one research was conducted by pi-labs where top ten victims of deepfakes was given wherein celebrities to public figures, influencers faced deepfake menace. "This year saw a surge in deepfakes due to easy-to-use AI tools capable of replicating real digital content within seconds. Specialized apps now generate deepfake videos, clone audio, and refine details with voice modulation and lip-syncing."[9] This list is topped by Rashmika Mandanna, Alia Bhatt, Rajat Sharma, the New Anchor, Ratan Tata[10], Sachin Tendulkar[11], Mukesh Ambani, RBI Governor Shaktikanta Das, cricketer Virat Kohli, and many others, who are facing the misuse of AI and victimised by deepfakes. One "pi-labs report, on digital deception epidemic: 2024

[5]McAfee Reports, "Shah Rukh Khan, Alia Bhatt, and Elon Musk Top McAfee India's 2025 'Most Dangerous Celebrities: Deepfake Deception List", Available at https://www.mcafee.com/en-in/consumer-corporate/newsroom/press-releases/2025/20251124.html#:~:text=India%2C%2024%20November%202025%20%E2%80%94%20McAfee,%2Dhave%E2%80%9D%20gadgets%20and%20supplements (last visited on April 6, 2026).
[6] *Ibid.*
[7] Roshni Shekhar, "SRK, Alia, Musk Lead 2025's Most Abused Deepfake List", *Rediff*, (November 15, 2025) available at https://m.rediff.com/news/report/srk-alia-musk-lead-2025s-most-abused-deepfake-list/20251115.htm#:~:text=McAfee's%20findings%20show%20that%20younger, Source (last visited on April 6, 2026).
[8] Pradip G Sagar, "Celeb impersonation to digital scams, how Indians are in deepfake dragnet", *India Today,* available at https://www.indiatoday.in/india-today-insight/story/celeb-impersonation-to-digital-scams-how-indians-are-in-deepfake-dragnet-2794626-2025-09-28, (last visited on April 6, 2026).
[9] Kahekashan, "pi-labs Unveils 2024's Top 10 Victims of AI Deepfakes: From Celebrities to Power Players", *The Hans India,* available at https://www.thehansindia.com/tech/pi-labs-unveils-2024s-top-10-victims-of-ai-deepfakes-from-celebrities-to-power-players-936426, (last visited on April 6, 2026).
[10] Sangeeta Ojha, "From Ratan Tata, Sachin Tendulkar to Madusudan Kela: 9 well-known personalities who were victims of deepfake videos", *Live Mint,* (14 March 2024) available at https://www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar-to-madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos-11710307982420.html, (last visited on April 6, 2026).
[11] *Ibid*.

on deepfake fraud's toll on India reveals a 550% increase in deepfake-related cybercrime cases since 2019, highlighting their growing impact. It is stated in this report that "Deepfakes are no longer just a technical issue—they undermine trust in the information we consume online. Addressing this requires concerted efforts on multiple levels."[12]

During 2nd voice of Global South Summit PM Modi raised serious concerns on deep fake videos and AI for creating misleading content. The recent video of PM Modi was gone viral, where he was doing garba.

"Union Minister Rajeev Chandrasekhar said that it is a "legal obligation" for online platforms to prevent the spread of misinformation. "Remove any such content when reported within 36 hours of such reporting and ensure expeditious action, well within the timeframes stipulated under the IT Rules 2021, and disable access to the content or information."[13]

III. IMPACT OF DEEPFAKE- CREATES MISINFORMATION TO THE PUBLIC AND HARASSMENT TO THE VICTIM

There are multiple cases and examples where people fall prey to deepfake activities, and follow, invest in a fake investment plans, believing it to be real. It is a clear breach of trust of a person, but who should be responsible for it- the victim himself, by deepfake activity or the perpetrator who has committed multiple frauds by making a deepfake image or video. To answer this, we need to look into some cases filed in the court.

Aishwarya Rai Bhachan vs Aishwaryaworld.com & Ors. [14] This case deals with the protection of personality and publicity rights in the digital space. The plaintiff is a well-known figure in the country. She approached the court against the unauthorized websites and online platforms, using her name, image, and identity for commercial gain without consent. The court opined that this kind of use amounts to infringement of personality rights, passing off, and potential violation of privacy, especially where it misleads the public into believing endorsement or association. The court restrained intermediaries to misuse, remove infringing content, and comply with due diligence. The hon'ble Delhi High Court held that the celebrities have enforceable rights over their name. likeness, and reputation in cyberspace and they can challenge unauthorized exploitation. If these rights are violated, that attracts legal liability under the law.

We have another similar case of Anil Kapoor[15], Bollywood actor on personality rights. In this case Delhi High Court also recognized the celebrity personality rights in the digital era. The plaintiff filed the case wherein protection was sought against unauthorized use of his name,

[12] *Supra* note 9
[13] Marya Shakil, "Recently Saw A Video...": PM Raises Concern Over Deepfakes", *NDTV News*, (November 17, 2023), Available at https://www.ndtv.com/india-news/pm-narendra-modi-says-deepfake-a-big-concern-asked-chatgpt-team-to-give-deepfake-warning-in-content-4581834 (last visited on April 28, 2026)
[14] CS(COMM) 956/2025, dated 9 September 2025
[15] Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

image, voice, likeness and distinctive attributes, which include his style and persona. This order was passed in favor of the plaintiff and against the various entities, including commercial endorsement by entities, merchandise and AI Deepfake content. The court specifically stated that the personality rights of a celebrity have a commercial value and the same is protectable under the doctrines of publicity rights, right to privacy. The court not only restraint the defendants but also unknown parties from misusing his identity in any form. The court directed all the intermediaries to take down such content that involves in digital manipulation and unauthorized endorsement. This judgement is significant where personality rights are extended beyond traditional misuse to cover emerging technologies like AI-generated content and deepfakes.

Amitabh Bachchan v. Rajat Nagi ,[16] In another example of the protection of personality rights. Plaintiff filed the case for permanent injunction against the unauthorised use of his name, voice, image, and his persona by various entities, including websites, applications, and merchandise sellers exploiting his identity for commercial gain.

There is another important case, among others, Raj Shammai [17] personality rights case. He, in current times, is a famous podcaster and influencer in India. He filed a case claiming protection of his personality rights and an injunction against the unauthorized use of his name, voice, image, and online persona by a third party. The issue includes the misuse of his persona over advertisements, social media promotions, and AI – generated or misleading content without consent. The court held that if the influencer has such an identity that acquires commercial value, then its unauthorized use through impersonation, deepfake, or endorsements can attract legal liability.

After careful analysis of the issues raised in the petitions of the petitioners showed how deepfakes impacted their reputation and personality rights which creates misinformation. For claiming their right to privacy, they went to the high court to save their personality rights and reputation. It is also noticed that personality rights jurisprudence in India is expanding, which also includes the modern online personalities and emerging technologies. In all the above cases, the hon'ble court passed the order in favor of the plaintiff by providing protection to his or her personality.

IV. AI APPS USED FOR IMAGE GENERATION

There are multiple apps from which deepfake pictures and videos are being created. Though these apps might have been developed for entertainment purposes, people start misusing the useful things. Following is the list of applications.

[16] (2022) 6 HCC (Del) 641
[17] CS(COMM) 1233/2025 decided on 17 November 2025

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

APP	CATEGORY	FUNCTIONALITY
Stable Diffusion	AI Image Generation Systems	Generate entirely new images based on textual prompts
Midjourney	AI Image Generation Systems	Generate entirely new images based on textual prompts
FaceApp	Deepfake Face-Swapping Technologies	Deep learning models to map and replace facial features
Reface	Deepfake Face-Swapping Technologies	Deep learning models to map and replace facial features
PicsArt	Traditional Image Editing and Morphing Tools	Manual or assisted alteration of visual content
DALL·E	AI Image Generation Systems	Generate entirely new images based on textual prompts
DeepFaceLab	Deepfake Face-Swapping Technologies	Deep learning models to map and replace facial features
FaceSwap	Deepfake Face-Swapping Technologies	Deep learning models to map and replace facial features
Adobe Photoshop	Traditional Image Editing and Morphing Tools	Manual or assisted alteration of visual content
Snapseed	Traditional Image Editing and Morphing Tools	Manual or assisted alteration of visual content
Chatgpt	Advanced AI chatbot	Generate text, image, and audio as required, answer queries

V. REGULATORY FRAMEWORK

Dealing with deepfake-related cybercrime is regulated under existing IT and criminal laws but many countries lack specific laws pertaining to deepfakes. India is also one of those countries. The framework we have, that rely on cybercrime, privacy rights, fraud, cyber bullying,

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

covering other issues, but deepfake as a specific issue is not given in any law. Also, the regulatory framework has many challenges, like privacy and consent as deepfake violates individual rights, misusing likeness without consent, and political manipulation, where information is used as misinformation for electoral interference. Not only this, the burden of proof is the major challenge for the regulatory framework, where in courts prosecution struggle with proving the intent and authenticity of the crime committed. Another major issue is cross-border issues and jurisdiction, as cybercrime is a transnational crime, deepfake crimes often transcend jurisdiction, which, of course, complicates the implementation process. The purpose behind these deepfake activities is very clear; it is done to commit defamation, harassment, misinformation for unlawful gain and financial loss. The following are the laws that we have:

In India

1. Information Technology Act 2000[18]
2. BNS
3. Digital Personal Data Protection Act (DPDP Act)
4. Constitution of India Article 21

Brief Glance at Regulatory Framework –

Laws under IT Act 2000	**Provision**
Section 66C	Identity theft
Section 66D	Cheating by personation
Section 66E	Violation of privacy
Section 67 AND 67A	Publishing obscene content

Laws under Bhartiya Nyaya Sanhita 2023 (BNS)

Laws under BNS	**Provision**
Section 356, Defamation	Fake images harming an individual's reputation, online defamation and through digital content
Section 318, Cheating	Cheating by deception, fraud and causing harm to body, mind, and reputation

[18] Sommya Kashyap, "Deepfakes in India: A Legal Analysis of Emerging Challenges and Regulatory Framework", *Law Article*, (September 9, 2025), available at https://lawarticle.in/deepfakes-in-india-a-legal-analysis-of-emerging-challenges-and-regulatory-framework/ (last visited on April 28, 2026)

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

Section 336, Forgery	Manipulated images, false documents, digital forgery and impersonation
Section 79, Outraging modesty	Words, gestures, sounds, objects or privacy intrusions intending to insult women's modesty
Section 77, Voyeurism	Non-consensual sharing of intimate images

Laws under DPDP Act, 2023

The DPDP Act does not expressly use the term "deepfake", but it indirectly regulates deepfake images by putting rules for consent, personal data protection, and accountability. Like, no personal data can be used without the person's consent. Personal data includes face, voice and image of a person. For getting the consent, it should be free, informed, specific, and unambiguous consent. If someone creates a fake image of a person without consent, DPDP Act 2023 mentions it as an illegal processing of personal data, and it attracts penalties under the Act.[19]

DPDP Act, puts liability on platforms and creators that all the platforms and AI companies are advised to take reasonable security safeguards and prevent the misuse of personal data. If any data breach is done, they can be held liable for this breach, and platforms or AI companies cannot hide themselves behind the user agreement clause. The Consent should be from the person whose data is misused.

The DPDP Act is inspired by the fundamental rights, such as the right to privacy and cybersecurity. Every victim has the right to the removal of content, fake images used online or on social media platforms. The victim has a right to approach the data protection board or the court.[20] Penalty provisions are also given under the DPDP Act which can be from 50 Crores -250 Crores fine[21]on the failure to protect personal data. This deepfake activity is the most serious crime which done against the consent of the victim; thus, it falls under the highest bracket of the penalties of the Act.

Comparison of Deepfake Laws in the USA and the European Union(EU) in Brief

This comparison between the USA, EU, and India pertaining to Deepfake laws is also necessary at this juncture. What kind of law do other countries have to deal with this deepfake menace?

[19] Press Information Bureau, Government of India, "India well-equipped to tackle evolving online harms and cyber crimes; Government to Parliament", 2025, Available at https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2154268&reg=3&lang=2, August 8, 2025

[20] Anahad Narain, "Penalties under the DPDP Act, Legality", Available at https://www.consent.in/blog/penalties March 12, 2024

[21]Schedule to The Digital Personal Data Protection Act 2023 Available at https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue S1,* 2026
Gurugram University Conference : 09-10 April 2026
Website: https://ceapress.org

In the USA

1. State laws in Texas and California criminalize deepfakes in non-consensual pornography and elections.
2. Foreign Trade Commission against deepfakes under consumer protection laws
3. Policy Gap, which is visible here, is that there is no Federal deepfake law

In the European Union

1. AI Act 2024 provides obligations for transparency in synthetic content and labeling of manipulated content
2. Policy Gap in the EU is that it has no uniform implementation

VI. CYBER SECURITY FROM DEEPFAKE: AS A HUMAN RIGHT

"Human rights are the basic rights that are inherent to all human beings, which are protected by the UDHR."[22] Basic fundamental rights are also human rights[23], like the right to live, the right to dignity, the right to live a dignified life[24]according to the Constitution of India. Cybersecurity consists of all the technologies,[25]where protection of individuals, their machines, networks, and data programs[26] from unauthorized access, digital attack, or any kind of damage committed online. We call it cybercrime if any perpetrator uses a computer, network or machine as a tool to commit offences, such as fraud, identity theft, etc.[27] As an individual, a person can be harmed by online scams for financial loss, loss of reputation, [28]and by morphed pictures and videos circulated for misinformation and undue benefits. Criminal jurisprudence clearly mentions that wrongful gain is a crime where a gain is made by unlawful means of property to which the person is not legally entitled[29]. Causing a financial loss to an individual that causes harm to an individual is also a wrongful loss for wrongful gain. Which attracts criminal liability. Thus, it requires the state's action to protect its individuals from cybercrime committed in cyberspace. But the question here is whether the cybersecurity of an

[22] Universal Declaration of Human Rights, available at https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf
[23] European Union Agency for Fundamental Rights, "What are fundamental rights?", available at https://fra.europa.eu/en/content/what-are-fundamental-rights
[24] Peace, Dignity and Equality on a Healthy Planet, United Nations, Available at https://www.un.org/en/global-issues/human-rights
[25] Nicholas Patterson, "What is Cybersecurity and Why is It Important?" Available at https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security, (last visited on April 6, 2026).
[26] Department of Information Technology, Malla Reddy College of Engineering & Technology, Available at https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20(R18A0521).pdf
[27] Chandigarh Police, "Cybercrime", Available at https://portal.chandigarhpolice.gov.in/LawRulesRegulation/CyberCrime
[28] Nik Hynek, Beata Gavurova, et. all, "Risks and benefits of artificial intelligence deepfakes: Systematic review and comparison of public attitudes in seven European Countries," *Journal of Innovation & Knowledge*, Volume 10, Issue 5,2025, ISSN 2444-569X, available at https://doi.org/10.1016/j.jik.2025.100782. (https://www.sciencedirect.com/science/article/pii/S2444569X25001271)
[29] Section 2(37), Bharatiya Nyaya Sanhita.

individual is a fundamental right or a human right of a person. As today, nobody can live without internet or we can say that everyone has right to access technology and take benefit but out of these benefits if something wrong is committed to an individual what will happen. The state has a duty to protect its citizens. "Right to Privacy in legal terms means "no one shall be subject to arbitrary interference with his/ her privacy, home, family, nor be subjected to attack on his/her reputation and honor." Right to Privacy has also been recognized as a human right under Article 12 of the Universal Declaration of Human Rights Act, 1948."[30] It can be said that if the right to reputation is a fundamental right and somewhere it covers the aura of human rights, then protection from deepfake images may come into the jurisprudence of human rights.

Policy Gap

No deepfake-specific laws are available in India, thus, it is required that the government come up with a specific legislation to deal with these deepfake concerns. DPDP Act 2023 is the law that is specifically for digital personal data protection, but it protects only personal data from issues. It does not mention the deepfakes of images and videos. Which is in need of an hour. The burden of proof, which is the major challenge for the regulatory framework, proving the intent and authenticity of the crime, cross-border issues, and jurisdiction are the necessary aspects to be looked into. As per the policy gap, we require explicit laws for dealing with the deepfake issue. International cooperation is also required for transnational deepfake cases. Mandatory watermarking or labeling is required for every AI-generated deepfake picture, as these apps are causing more harm than the benefits to an innocent citizen. To fill the gap in policy, it is also required to develop stronger digital evidence collection standards with specialized and tech-savvy prosecution officers and police officials for the collection of evidence in cybercrime and deepfake cases.

References

1. Abhishek Sheoran, YouTube To Penalise Content Creators Who Do Not Mention Use Of Deepfake In Videos, available at https://www.thedailyjagran.com/world/youtube-to-penalise-content-creators-who-do-not-mention-use-of-deepfake-in-videos-10114038, 15 November 2023
2. Aishwarya Rai Bhachan vs Aishwaryaworld.com & Ors. CS(COMM) 956/2025, dated 9 September 2025
3. Alia Bhatt, Rashmika Mandanna, Ranveer Singh, Virat Kohli, Sreeleela, Payal Gaming: Indian celebs who became victims of deepfake Available at https://www.dnaindia.com/entertainment/photo-gallery-payal-gaming-sreeleela-alia-bhatt-rashmika-mandanna-amitabh-bachchan-ranveer-singh-virat-kohli-katrina-kaif-kajol-indian-celebs-who-became-victims-of-deepfake-ai-generated-videos-photos-fake-clips-3194030

[30] Pallavi Sharma, "Right To Privacy: The Impact Of Cyber Security On An Individual", *International Journal of Engineering, Management and Humanities (IJEMH)*, Volume 4, Issue 3,(May-June, 2023) pp: 129-136

4. Altuncu E, Franqueira VNL, Li S. "Deepfake: definitions, performance metrics and standards, datasets, and a meta-review" *Front Big Data.* 2024 Sep 4;7:1400024. doi: 10.3389/fdata.2024.1400024. PMID: 39296632; PMCID: PMC11408348.
5. Alex Singla, Alexander Sukharevsky, Lareina Yee, and Michael Chui, with Bryce Hall, representing views from Quantum Black, AI by McKinsey. The state of AI: How organizations are rewiring to capture value, March 12, 2025 | Survey
6. Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914
7. Anahad Narain, "Penalties under the DPDP Act, Legality", Available at https://www.consent.in/blog/penalties, March 12, 2024
8. Amitabh Bachchan v. Rajat Nagi 20226 HCC (Del) 641
9. A. Shaji George, & A. S. Hovan George. (2023). Deepfakes: The Evolution of Hyperrealistic Media Manipulation. *Partners Universal Innovative Research Publication*, *1*(2), 58–74. https://doi.org/10.5281/zenodo.10148558
10. Bengaluru Police Launches Helpline To Combat Deepfake Menace: Here's All Details, India.com News Desk, available at https://www.india.com/news/india/bengaluru-police-launches-helpline-to-combat-deepfake-menace-heres-all-details-6512448/, 18 November 2023.
11. Bharatiya Nyaya Sanhita 2023.
12. CAROLINA ROSSINI AND NATALIE GREEN, CYBERSECURITY AND HUMAN RIGHTS, PUBLIC KNOWLEDGE
13. Chandigarh Police, "Cybercrime", Available at https://portal.chandigarhpolice.gov.in/LawRulesRegulation/CyberCrime
14. Department of Information Technology, Malla Reddy College of Engineering & Technology, Available at https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20(R18A0521).pdf
15. Deepfake shock : Nirmala Sitaraman Reveals fake videos of herself online, warns of AI's Dark side, Times of India available at https://timesofindia.indiatimes.com/videos/news/deepfake-shock-nirmala-sitharaman-reveals-fake-videos-of-herself-online-warns-of-ais-dark-side/videoshow/124361288.cms, 7 October 2025
16. Dr. A. Shaji George, & A. S. Hovan George, "Deepfakes: The Evolution of Hyper realistic Media Manipulation", *1*(2), *Partners Universal Innovative Research Publication*, 58–74. (2023) https://doi.org/10.5281/zenodo.10148558
17. European Union Agency for Fundamental Rights, "What are fundamental rights?", available at https://fra.europa.eu/en/content/what-are-fundamental-rights
18. Explained: How ChatGPT Algorithm Is Used to Make Deepfakes, NDTV News Desk, available at https://www.ndtv.com/india-news/explained-how-chatgpt-algorithm-is-used-to-make-deepfakes-4582350, 17 November 2023
19. From Ratan Tata, Sachin Tendulkar to Madusudan Kela: 9 well-known personalities who were victims of deepfake videos, Available at https://www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar-to-

madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos-11710307982420.html

20. Janhvi Kapoor Recalls Seeing Her 'Morphed Image On Porn Site': "This Is The Cost You've To Pay", NDTV Movies News Desk, Available at https://www.ndtv.com/entertainment/janhvi-kapoor-on-seeing-her-morphed-image-on-porn-site-at-15-it-upsets-me-11313131, 5 April 2026
21. Jeet Padhya, "AI is a Tool, Not a Replacement: How Artificial Intelligence Amplifies Human Capability", *available at* https://medium.com/@jeetpadhya35/ai-is-a-tool-not-a-replacement-how-artificial-intelligence-amplifies-human-capability-7a798ba864d2 (last visited on April 6, 2026).
22. Kahekashan, "pi-labs Unveils 2024's Top 10 Victims of AI Deepfakes: From Celebrities to Power Players", *The Hans India,* available at https://www.thehansindia.com/tech/pi-labs-unveils-2024s-top-10-victims-of-ai-deepfakes-from-celebrities-to-power-players-936426, (last visited on April 6, 2026).
23. Marya Shakil, "Recently Saw A Video...": PM Raises Concern Over Deepfakes", *NDTV News*, (November 17, 2023), Available at https://www.ndtv.com/india-news/pm-narendra-modi-says-deepfake-a-big-concern-asked-chatgpt-team-to-give-deepfake-warning-in-content-4581834 (last visited on April 28, 2026)
24. McAfee Reports, "Shah Rukh Khan, Alia Bhatt, and Elon Musk Top McAfee India's 2025 'Most Dangerous Celebrities: Deepfake Deception List", Available at https://www.mcafee.com/en-in/consumer-corporate/newsroom/press-releases/2025/20251124.html#:~:text=India%2C%2024%20November%202025%20%E2%80%94%20McAfee,%2Dhave%E2%80%9D%20gadgets%20and%20supplements (last visited on April 6, 2026).
25. McAfee Report The World's Most Deepfaked Celebrities Revealed Available at https://www.mcafee.com/blogs/internet-security/the-stars-scammers-love-most-mcafee-reveals-worlds-most-deepfaked-celebs/
26. Nicholas Patterson, "What is Cybersecurity and Why is It Important?" Available at https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security, (last visited on April 6, 2026).
27. Nik Hynek, Beata Gavurova, et. all, "Risks and benefits of artificial intelligence deepfakes: Systematic review and comparison of public attitudes in seven European Countries," *Journal of Innovation & Knowledge*, Volume 10, Issue 5,2025, ISSN 2444-569X, available at https://doi.org/10.1016/j.jik.2025.100782.
28. No End To Deepfake Menace | How Safe Are We From Deepfakes In Real Life? Available at https://www.timesnownews.com/videos/times-now/newshour/no-end-to-deepfake-menace-how-safe-are-we-from-deepfakes-in-real-life-newshour-agenda-video-105298941, 17 November 2023
29. Pallavi Sharma, "Right To Privacy: The Impact of Cyber Security On An Individual", *International Journal of Engineering, Management and Humanities (IJEMH)*, Volume 4, Issue 3,(May-June, 2023) pp: 129-136
30. Peace, Dignity and Equality on a Healthy Planet, United Nations, Available at https://www.un.org/en/global-issues/human-rights

31. Pradip G Sagar, "Celeb impersonation to digital scams, how Indians are in deepfake dragnet", *India Today,* available at https://www.indiatoday.in/india-today-insight/story/celeb-impersonation-to-digital-scams-how-indians-are-in-deepfake-dragnet-2794626-2025-09-28, (last visited on April 6, 2026).
32. Press Information Bureau, Government of India, "India well-equipped to tackle evolving online harms and cyber crimes; Government to Parliament", 2025, available at https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2154268&reg=3&lang=2, August 8, 2025.
33. Raj Shammai CS(COMM) 1233/2025 decided on 17 November 2025
34. Roma Patel, Robinson & Cole LLP, Lights, Camera, [AI] Action- India's Recent Celebrity Deepfake Lawsuits, 31 December, 2025
35. Roshni Shekhar, "SRK, Alia, Musk Lead 2025's Most Abused Deepfake List", *Rediff*, (November 15, 2025) available at https://m.rediff.com/news/report/srk-alia-musk-lead-2025s-most-abused-deepfake-list/20251115.htm#:~:text=McAfee's%20findings%20show%20that%20younger, Source (last visited on April 6, 2026).
36. Sangeeta Ojha, "From Ratan Tata, Sachin Tendulkar to Madusudan Kela: 9 well-known personalities who were victims of deepfake videos", *Live Mint,* (14 March 2024) available at https://www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar-to-madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos-11710307982420.html, (last visited on April 6, 2026).
37. Schedule to The Digital Personal Data Protection Act 2023 Available at https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
38. Sommya Kashyap, "Deepfakes in India: A Legal Analysis of Emerging Challenges and Regulatory Framework", *Law Article*, (September 9, 2025), available at https://lawarticle.in/deepfakes-in-india-a-legal-analysis-of-emerging-challenges-and-regulatory-framework/ (last visited on April 28, 2026).
39. Surge of Deepfake AI Videos Targets Indian Actresses, Sparks Government Action Available at https://oecd.ai/en/incidents/2023-11-15-ed57
40. Tahir Qureshi, "I was seen singing a Garba song': PM Modi Raises Serious Concern On Deepfake, AI After His Video Singing Garba Goes Viral", available at https://www.india.com/news/india/pm-narendra-modi-deepfake-video-raises-serious-concern-misuse-of-artificial-intelligence-chatgpt-bjp-diwali-rashmika-mandanna-katrina-kaif-kajol-6509165/, 17 November 2023.
41. United Nations Office on Drugs and Crime, SHERLOC-Sharing Electronic Resources and Laws on Crime, Available at https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-2/key-issues/computer-related-offences.html
42. Universal Declaration of Human Rights, available at https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf
43. Vikas Yadav, Deepfake Concern: Govt To Meet Google, Meta, Other Social Media Firms To Address AI Crisis; Here's What IT Minister Said, available at https://www.thedailyjagran.com/technology/ai-deepfake-concern-indian-government-

to-meet-google-meta-social-media-firms-to-address-ai-crisis-what-ashwini-vaishnaw-it-minister-said-10114815, 19 November 2023.