REGULATING DEEPFAKES IN INDIA: A LEGAL AND ETHICAL ANALYSIS OF MISINFORMATION IN THE AGE OF AI

Asim Mustafa Khan, Jamia Millia Islamia

ABSTRACT

The rapid rise of deepfake technology AI-generated synthetic media that alters audio, video, or images creates immediate legal and ethical concerns for India's digital society. Deepfakes impair individual privacy, consent to use, reputation, and national security and also increase misinformation, disinformation, and electoral tampering. The Indian legal architecture, including the Information Technology Act and Indian Penal Code, remains responsive and piecemeal, and therefore does not provide adequate redress for the complex harms posed by deepfakes.

This paper uses a doctrinal and comparative legal analysis approach by analysing Indian laws in contrast to regulatory responses in the United States, European Union, and China. It provides an overview of judicial responses in India in addition to the formation of digital personality rights, but also notes the lack of a coordinated legislative approach.

The paper concludes by calling for a prospective rights-based regulatory approach whether via watermarking, AI responsibility, platform responsibility, or public digital literacy frameworks. This view is based on Indian constitutional values with relation particularly to Articles 19 and 21 and defending access to innovation and freedom of expression, while preserving safeguards against digital harms. The research concludes by stating that without reform that anticipates the deepfake threat and builds public trust in the information digital realm, India runs the risk of lagging further behind in responding to the changing threat from deepfakes.

Keywords: Deepfakes, Misinformation, Disinformation, Artificial Intelligence (AI), Generative Adversarial Networks (GANs), Non-consensual pornography, Synthetic media, Identity theft

Background and History

The fast-paced technology development of Artificial Intelligence (AI) specifically generative technologies has created "deepfakes", or realistic synthetic media manipulated audio, video, or images through deep learning algorithms. Initially developed for innovation or harmless amusement, deepfakes have since been weaponized for purposes such as misinformation, political propaganda, cyberbullying, identity theft, and non-consensual pornography. India's vast population and widespread digital adoption make it particularly vulnerable to synthetic media threats.[1] The proliferation of smartphones along with low cost internet, and the fact that more of our population is now socially engaged than ever before has fueled the consumption of synthetic content.[2] The pattern of misinformation spreading faster than detection and disruption is troublesome since it challenges individual rights, democratic processes, national security, and public trust. India legally has no overarching legislation or policy directly focusing on deepfakes. There are currently laws offered as infringement remedies for deepfakes such as the Information Technology Act, 2000, the Indian Penal Code, 1860 or under certain sections of the Copyright Act, 1957. However, these broad legal frameworks are not specifically tailored to address the unique harms posed by AI-generated misinformation. In addition, ethical concerns around consent, digital identity, and the right to privacy as reiterated by the Supreme Court's landmark Puttaswamy judgment (2017) demand a more sophisticated regulatory approach.

The gap between the capabilities of the generators and detection technology continues to grow with advances in deepfake technology, creating the urgency for India to develop a unified ethical and legal framework that balances the benefits of innovation and freedom of expression against accountability, privacy and protection against harm

Research Methodology

In this study, I take a doctrinal and analytical approach, analyzing existing Indian legal provisions, judicial decisions, and constitutional principles with relevance to deepfakes and misinformation. I utilize comparative legal analysis of international legal frameworks (EU,

[1] Internet and Mobile Association of India, *Digital in India Report 2023*, available at https://www.iamai.in (last visited on 3 July 2025).
[2] Telecom Regulatory Authority of India, *Monthly Performance Report for Internet & Broadband* (2023), available at https://trai.gov.in (last visited on 3 July 2025).

U.S., China) and cases of significant deepfake incidents involving public figures. Through qualitative content analysis, and drawing on available government advisories, policy drafts and judgments, as well as legal treatises, I analyse the legal, ethical and social perspectives of deepfakes and misinformation. Although I do not collect my own empirical data, I try to ensure depth and significance through secondary sources and analyse to triangulate and corroborate the legal, ethical and social perspectives.

Research Problem

The increase of deepfakes has revealed major gaps in the legal framework in India, including the absence of recent provisions to address the epidemic misuse of AI-generated content as misinformation, identity theft, and non-consensual media. This research will explore how India might seek to create a strong, architecture-based legal solution that aims to balance variance and individual rights with digital responsibility and free speech.

Hypothesis

India's continued reliance on pre-existing laws such as the IT Act and IPC is inadequate without distinct technology positive legal frameworks to regulate the abuse of deepfake images. Without a specialized, rights-oriented law, complementing AI detection, intermediary accountability, and civic awareness will be limited in its ability to protect the democratic cycle, individual rights, and the integrity of the digital products.

Research Question

“Is it possible for India to establish a good regulatory framework that regulates deepfakes but also respects rights enshrined in the constitution and the common good of democracy?”

Chapter II

Review of Literature

2.1 Introduction

Deepfake technology is now a major emergent digital threat. A number of interdisciplinary literatures examining the risks associated with synthetic media has emerged comprising various

valuable perspectives including legal theory, technological inquiry, ethics, and public policy. This chapter integrates selected significant contributions which will assist in informing legal and ethical analysis of the relevant issues globally, and within India.

2.2 International Legal and Policy Literature

Amongst the initial legal problems associated with deepfakes, were noted by a small group of scholars. The legal scholars Robert Chesney and Danielle Citron argued in their article "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" in the California Law Review, (2019) 107(6) 1753, that the existing laws that concern defamation, privacy, and electoral interference, do not adequately address the fraudulent nature of synthetic media.

Within the EU, Veale and Zuiderveen Borgesius (2021) promisingly delved into the legal regimes, by examining the EU AI Act and Digital Services Act through a constitutional and human rights framework, which involved a focus on risk-based AI classifications and transparency and labeling strategy, to help contain misinformation produced through AI.

Lastly, in China some regulatory scholars (e.g., Zhang, 2023) examine the regulation through Deep Synthesis Provisions which have strict algorithm auditing, tracing and also watermarking, which if performed effectively, will incorporate government surveillance contrary in some ways to liberal democratic state governance.

2.3 Indian Legal and Scholarly Discourse

Legal scholarship on deepfakes is still coming into its own in India, but there are a few important commentaries from think tanks and policy bodies, including:

Vidhi Centre for Legal Policy: The briefing 'AI and the Indian Legal Landscape' (2022) makes clear that existing regimes, like the IT Act and the IPC, do not adequately cover altered audiovisual works in relation to enduring harms caused by AI.

ORF: Through their report, 'The Deepfake Dilemma in India' (2023), they have highlighted the gendered and communal harms of deepfakes.

Carnegie India: Their work on AI governance shows the importance of transparent algorithms and independent regulation.

Similarly, there are judicial comments in the public law domain and law journal articles advocating for personality rights that will expand to allow for addressing any misuse of likeness and identity in AI-generated content.

2.4 Ethical and Human Rights Considerations

Deepfake technology creates disturbing ethical challenges around autonomy, consent, privacy and power relationships in the online environment. At a conceptual level the deepfake presents a challenge to informational autonomy, i.e., the right to determine how an individual can interact with and control their identity, image or likeness in digital space. This is particularly troubling in the Indian context as a deepfake involves breaches of constitutional rights like the Article 21 right which now include privacy and dignity as part of the right to life and personal liberty through implied judicial expansion, most famously in Justice K.S. Puttaswamy v. Union of India.

UNESCO's Recommendation on the Ethics of Artificial Intelligence, issued in 2021, recognizes core ethical values relevant to AI systems such as transparency, accountability, human dignity and the principle of "do no harm". The Indian law has incorporated some of these principles but not fully. Additional researchers (Wachter & Mittelstadt, 2019) included a right to "reasonable inferences" as a new form of digital dignity and applying this to AI-generated manipulation, that is the representation of individuals algorithmically, possibly without consent. Deepfakes - especially in non-consensual sexual imagery, satire or close fakes - further disrupt this balance and impose potential emotional distress, reputational harm and psychological trauma.

Moreover, the effects of deepfakes also disadvantages women, public figures, and marginalized groups in ways that perpetuate existing structural inequalities. The ethical dilemma cannot simply be a private concern, as there are shared costs or effects, like public trust, fairness in elections, and community unrest. And the effects of the technology are ethically hazardous without the means to give or obtain consent, no accountability for producers, and no recourse for victims. In a democratic society like India, it is important to honor the intersection between the legal and the ethical issues while also considering that the right to free speech under article 19(1)(a), and the right to dignity and public order under article 19(2) can be harder to navigate. The ethical regulation must also be protective against the potential for state overreach, which would occur if a regulation of deepfakes becomes a tool of repression, whereby dissent or

justifiable critique of state action become censored. As such, ethical AI governance in India must be built on dimensions of (democratic) accountability, gender justice, and the human-rights based design.

2.5 Gaps in the Literature

While awareness of these issues is increasing, the following gaps still exist: Doctrinal analysis that links deepfakes directly to Indian constitutional law. Empirical or policy literature on how synthetic media can lead to electoral interference. No national legal framework governing deepfaking across the country. Little academic attention given to intermediary liability and platform responsibility.

2.6 Conclusion

The review of the literature shows a global recognition of deepfakes being a legal and ethical frontier. Countries such as the U.S., EU, and China have now begun stating policy responses, however, India's response has mostly been reactionary to global trends. The review provides justification for the country to adopt an anticipatory legal framework with constitutional safeguards, AI accountability, and user protection to preemptively address the threats posed by deepfakes.

Chapter III

Understanding Deepfakes and Misinformation

3.1 Introduction

The rise of deepfakes highly realistic but fabricated digital content presents newly complex problems for media claiming to be real, the dissemination of information, and maintaining public trust. By utilizing artificial intelligence, deepfakes continuously erase the boundary between reality and fabrication. This has consequences for politics, security, and individual rights.

3.1.1 Defining Deepfakes and Underlying Technology

Deepfakes, as synthetic media, are created with machine learning algorithms, such as

Generative Adversarial Networks. The technique of Generative Adversarial Networks was introduced by Goodfellow et al. (2014), and it consists of two networks: A generator that creates some fake content, and a discriminator that determines whether the content is fake or real. After training through many iterations, the included algorithms create convincing audio-visual content.[3]

There is also the possibility of using autoencoders of the deepfake development, which are used to learn a representation of facial movement, and to reconstruct this movement such as natural language processing models can learn the voice and text speaking patterns.[4]

3.2 Typology and Examples of Deepfakes

3.2.1 Video Deepfakes

These are potentially the most recognizable form in which an individual's face or expressions have tampered with, or possibly replaced altogether. Some interesting examples include concocted videoclips with politicians appearing to say controversial statements.[5]

3.2.2 Audio Deepfakes

Artificial intelligence-generated voice having an unthinkable likeness to an unknown individual's speaking mannerisms and preferences. In 2019, scammers used voice cloning to impersonate a CEO to fake a transaction.

3.2.3 Image-Based and Textual Deepfakes

Images of manipulated or entirely made-up people are called deepfakes and the latest advancements in AI allow users to generate fake written information such as fake news articles, compressed down to something a chatbot actually wrote.[6]

---

[3] Kietzmann, J., McCarthy, I. P., & Pitt, L. (2020). *Deepfakes: Trick or treat?* Business Horizons, 63(2), 135–146
[4]Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107(6) *California Law Review* 1753.
[5] *Vaccari, C and A Chadwick, 'Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News' (2020) 6(1) Social Media + Society.*
[6] Hern, A. (2023). *AI-generated disinformation is getting harder to detect, experts warn*. The Guardian. (last visited 3 July 2025).

3.3 Deepfakes in the Context of Misinformation and Disinformation

Deepfakes play a crucial role in both misinformation unintentionally shared false content and disinformation, which is shared with deliberate intent to deceive.[7]. Deepfakes create new challenges for fact checking, elevate levels of conspiracy theorizing and erode confidence in real media

In social media, deepfakes routinely become viral content before they are fact-checked, leveraging both algorithmic amplification and confirmation bias.[8] All the while, their role in digital propaganda will continue to expand while detection tools will continue to lag their creation.[9]

3.4 Societal and Political Impacts

3.4.1 Electoral Interference and Democratic Processes

Deepfakes pose an emerging risk to electoral integrity by facilitating convincingly fabricated representations at opportune moments to strategically influence the public. In situations where media literacy is low or political polarization is high, even small exposures can sway voter attitudes and behavior.[10].

3.4.2 National and International Security

Deepfakes from faked diplomatic communications to AI assisted information warfare are a new instrument for use in geopolitical conflict. Intelligence and defense operators are increasingly worrying about their use in psychological operations[11].

3.4.3 Violation of Individual Rights

Deepfake technologies are often used to make non-consensual pornography consistent with the

[7] Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe. (last visited on 3 July 2025).
[8] David Lazer et al., 'The Science of Fake News' (2018) 359(6380) *Science* 1094.
[9] Wardle, C. and Derakhshan, H., *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making* (Council of Europe, 2017).
[10] Dobber, T., Trilling, D., Helberger, N., and de Vreese, C. H., "Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?", (2021) 26(1) *The International Journal of Press/Politics* 69.
[11] *Patrick Tucker, 'Deepfakes and the New Disinformation War' Defense One (18 January 2019) https://www.defenseone.com/technology/2019/01/deepfakes-and-new-disinformation-war/154002/* (Last date visited on 3 July 2025)

experiences of many women and public figures. Victims, particularly public figures, often suffer reputational and psychological harm, with limited legal recourse available in many jurisdictions.[12]

3.4.4 Erosion of Epistemic Trust

Deepfakes contribute to what scholars term the 'liar's dividend' a situation in which even authentic content is dismissed as fake, leading to a general erosion of trust in digital evidence.[13]

3.5 Conclusion

In Chapter II, we talked about the immediate ethical concerns related to deepfakes and their relation to privacy, autonomy, and public trust, especially given India's limited legal protections for these issues. In the next chapter, we will examine the legal framework existing around deepfakes.

Chapter IV

Legal Landscape in India

4.1 Introduction

At present, there are no particular laws directly addressing deepfake related video. However, there are some existing laws that can be utilized to address the problems of deepfakes indirectly.

The Information Technology Act, 2000(IT Act 2000) is the primary legislation of India that establishes the law relating to cybercrime as well as electronic commerce. While the Act itself does not state deepfakes and its implications, some provisions of the Act deal with the problems of deepfake content and deception and misrepresentation such as identity theft, defamation, and obscenity.

4.1.1 Information Technology Act, 2000 (IT Act)

India's primary cybersecurity law includes several sections frequently used to address deepfake

[12]Deeptrace Labs, *The State of Deepfakes: Landscape, Threats, and Impact* (2019), available at https://www.deeptracelabs.com (last visited on 3 July 2025).
[13] Chesney, Robert and Citron, Danielle, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", (2019) 107 *California Law Review* 1753.

offenses:

Section	Offense	Applicability to Deepfakes	Penalty
66C	Identity theft (using someone's password or unique ID)	When deepfakes replicate biometric or credential information to impersonate someone	Up to 3 years imprisonment + ₹1 lakh fine
66D	Cheating by personation via computer/communication device	Deepfake videos or voice clones used to mislead or defraud	Up to 3 years imprisonment + ₹1 lakh fine
66E	Privacy violation publishing private images	Non-consensual deepfake pornography or intimate content	Up to 3 years imprisonment + ₹2 lakh fine
67 / 67A / 67B	Publishing obscene / sexually explicit electronic content; child pornography	Applies to erotic deepfakes, especially involving minors	S.67: up to 5 years & ₹10 lakhs fine; 67A: up to 7 years & ₹10 lakhs fine; 67B (child): up to 5–7 years & ₹10 lakh fine
43	Unauthorized access/damage to computer systems	When hacking or data theft is involved in creating deepfakes	Civil liability for damage up to ₹1 crore
66	Hacking unauthorized data modification	If deepfakes involve hacking personal devices or networks	Up to 3 years imprisonment + ₹5 lakh fine
69A	Blocking access to specified content	Enables MeitY to block deepfake-hosting platforms under legal order	
79 + IT Rules, 2021	Intermediary liability & safe-harbor regime	Platforms must promptly takedown user complaints (36 hrs); failure results in liability	

4.1.2 Provisions of BNS, 2023 Targeting Misinformation & Deepfakes

Deepfakes and related misrepresentations are specifically addressed by a number of provisions in India's new Bharatiya Nyaya Sanhita (BNS) 2023 (which goes into effect on July 1, 2024). This is a summary:[14]

Provision	Section	Key Focus	Explanation
False information/public mischief	**Section 153**	Spreading false or misleading information	Punishes those who disseminate untrue news, or statements that may encourage panic, disrupt public peace, or incite violence.
Deepfake misuse (digitally manipulated content)	**Section 356**	Forgery of electronic records	Targets the creation or communication of manipulated digital content (including deep fakes) intended to mislead or harm. Penalties are elevated for use resulting in cheating or defamation.
Identity theft and digital impersonation	**Section 337**	Digital fraud and impersonation	Punishes using a fake identity or a real person identity (including fake profiles from any of a variety of AI tools or deep fakes) to create fraud, lead someone astray, or damage their reputation
Obscene/sexually explicit deepfakes	**Section 74 & 75**	Obscenity and sexual offenses using AI	Criminalizes the act of creating or distributing obscene or sexually explicit digital content (e.g., AI generated porn) without consent.
Terror or panic via fake content	**Section 113**	Statements conducing to public mischief	Refers to deep fakes or disinformation, etc as publication systems that may cause panic; for example, false domestic terrorist alerts or other content causing hatred or panic.

[14] Government of India, *Bharatiya Nyaya Sanhita, 2023*, Ministry of Law and Justice, New Delhi (2023)

4.1.3 Navsari Deepfake of Prime Minister Modi (May 2025)

- **Incident:** A deepfake video of PM Modi in a hypothetical attack situation was shared in a WhatsApp group.

- **Legal outcome:** Mahendra Patel was charged under BNS Section 197 (1)(D) and 353 (1)(B) (public mischief), and the IT Act 66(C) (identity theft).[15]

4.1.4 Copyright Act 1957 Relevance to Deep Fakes[16]

Section	Relevance to Deepfakes
51	Prohibits unauthorized reproduction or distribution of copyrighted work; extends to intermediate users who profit from infringing contents.
57	Protects moral rights; allows authors to object to distortion even if not harmful deepfakes.
52	Finely stated, 'fair dealing' is limited a deepfake used to review content might be defensible, but malicious uses would not be protected.

In **Anil Kapoor v. Simply Life India & Ors**[17], decided, actor Anil Kapoor has sued various parties for unlawful commercial appropriation of his persona (name, name, image, voice, gestures, and phrases like "Jhakaas", including via AI-generated deepfakes and digital content). The Delhi High Court granted an ex parte injunction restraining the unlawful use and granted orders to delete the infringing content and transfer the domain names to Kapoor.

4.1.5. Constitution of India – Article 19 (freedom of speech and expression)

(1) All citizens shall have the right

(a) to freedom of speech and expression;

(b) to assemble peaceably and without arms;

(c) to form associations or unions or co-operative societies;

[15] 'Navsari Man Held for Sharing Deepfake Video of PM in WhatsApp Group', *The Times of India*, 16 May 2025.
[16] *The Copyright Act, 1957*, Act No. 14 of 1957, India Code (as amended by Act No. 27 of 2012).
[17] *Anil Kapoor v. Simply Life India & Ors.*, 2023 SCC Online Del 4532.

(d) to move freely throughout the territory of India;

(e) to reside and settle in any part of the territory of India;

(g) to practice any profession, or to carry on any occupation, trade or business.

(2) Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.[18]

These reasons apply directly to deepfakes and misinformation, especially when:

• Political consequences are manipulated through deepfakes (public order, integrity of India)

• Misinformation leads to communal violence or hate speech (public order)

• The content is obscene or harmful to morality

• The fraudulent information is defamatory.

In **Amitabh Bachchan v. Rajat Negi**[19], finding that the use of their likeness (a deepfake) infringed upon privacy and personality rights and Article 19(2) rights, specifically for commercial or defamatory appropriation.

4.2. Role of regulatory bodies

4.2.1 Ministry of Electronics & IT (MeitY)

Advisories to Intermediaries

On December 27, 2023, MeitY ordered platforms such as Meta and Google to track and restrict misinformation and deepfakes, powers it exercises through Rule 3(1)(b) of the Information

[18] The Constitution of India, Article 19(1)(a), read with Article 19(2).
[19] *Amitabh Bachchan v. Rajat Negi*, 2022 SCC Online Del 3625.

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[20]

On March 1, 2024, it ordered that generative AI content includes metadata or watermarks so that originators can be identified.[21]

4.2.2 Legal Instruments Used

Intermediaries, in accordance with the requirements of the Information Technology Act, 2000 and Information Technology (Intermediaries Guidelines) Rules 2021, may suffer penalties including jail terms up to three years and a fine of ₹1 lakh, if they do not remove impersonation deepfake or manipulated media within 24 hours.

The Information Technology Act, 2000, sections 66D, refers to impersonation carried out using digital devices.

4.2.3 Broader AI Governance

The MeitY is involved with the India AI Safety Institute (established Jan 2025) to develop AI ethical and safety standards[22]

Worked with UNESCO on AI readiness and ethical frameworks to enable the safe deployment of AI in India.

4.3. Election Commission of India (ECI)

4.3.1. Proactive Directives

The Election Commission of India (ECI) instructed political parties to remove deepfake/misinformation content in 3 hours of notice, warn individuals who raise this and give them report on repeated instances on May 6, 2024.

They specifically warned that they will treat AI deepfakes as already violating the IT Act, IPC,

[20] Ministry of Electronics and Information Technology, *Advisory on Deepfakes and Metadata Requirements*, Government of India, New Delhi (27 December 2023)
[21] Ministry of Electronics and Information Technology, *AI Content Advisory with Watermarking Requirement*, Government of India, New Delhi (1 March 2024)
[22] Ministry of Electronics and Information Technology, "AI Safety Institute Launch Press Release", Government of India, https://www.meity.gov.in (last visited on 3 July 2025).

Representation of People Act, and the Model Code of Conduct (MCC).[23]

4.3.2. Electoral Oversight & Response

In the 2024 General Elections, the ECI initiated ramped up monitoring sending officials and using keyword tools to detect misinformation flag and counter misinformation (such as deepfake videos of high-profile individuals.[24]

Legal cases and platform takedowns were initiated in high profile cases surrounding AI-generated content related to Amit Shah and others.

4.4. Recent amendments or proposed legislation

4.4.1 Karnataka's Draft Fake News Bill

The Karnataka government has presented the Karnataka Misinformation and Fake News (Prohibition) Bill, which would impose sentences of up to 7 years imprisonment for those spreading "fake news", to include AI generated misinformation, "anti-feminist" content, or any content that derives from superstition.

The bill's draft does not provide clear definitions for any of the key terms, causing concern regarding the potential of misuse and overreach. The draft mentions special courts, as well as regulatory committees. [25]

The state has decided on public consultation and feedback, but advocates are concerned that this could risk censorship of memes or legitimate mistakes.

4.4.2 Digital India Bill

The Digital India Bill will soon be released to supersede the current and inadequate Information Technology Act, 2000. Like many countries, we must grapple with consequences of developing technologies including artificial intelligence, deepfakes, and digital misinformation. The Bill,

[23] The Hindu Bureau, *"EC warns political parties against misuse of AI-based tools"*, **The Hindu**, New Delhi, June 28, 2024. (last visited 3 July 2025).
[24] Ishaan Tharoor, "India sieves online deluge, to stamp out disinformation in world's biggest election," *Reuters*, April 25, 2024. (last visited on 3 July 2025).
[25] Government of Karnataka, *Draft Misinformation and Fake News (Prohibition) Bill*, (June 2025) Ministry of Electronics and Information Technology, *Press Release on Digital India Bill Consultation*, PIB, New Delhi (March 2023) https://www.pib.gov.in/... (last visited 3 July 2025)

promulgated by the Ministry of Electronics and Information Technology (MeitY) proposes a regulatory framework by assigning regulatory incidence on digital platforms based on a size and risk continuum,[26] enhanced accountability for intermediaries and expanded user protections so as to confront dangers of harm that may come from the Internet, for example, cyberbullying, identity theft and AI-generated misinformation,[27] the establishment of an independent internet regulation body, the adoption of open and safe innovation principles; and details corresponding with the Digital Personal Data Protection Act, 2023[28] and other codifying legal its generations of the Bill, also provided extensive stakeholder consultations with civil society and industry perspectives, with the objective of meeting India's collective ambition to become a trusted provider in the global digital economy. [29]The Bill is a steady part of India's digitalization projects into 2030. As of mid-2025, the Bill is in the last stages of drafting and will be tabled in Parliament in a near future.

4.5 Conclusion

India's current legal framework is dispersed across various statutes and lacks the coherence needed to proactively address emerging deepfake challenges. The Digital India Bill and the BNS 2023, demonstrate some effort, but coherence and enforceability are lacking. Deepfakes will evolve and so must the law, moving away from a piecemeal way of working, to a systematic and proactive way of working. The next chapter of this project will look at how other international jurisdictions have begun to address the gap and allot what lessons India can learn from them.[30]

[26] Ministry of Electronics and Information Technology, *Press Release on Digital India Bill Consultation*, (March 2023), available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1905639 (last visited July 5, 2025).
[27] India Briefing, *Digital India Bill 2023: Key Provisions and Stakeholder Perspectives*, (Aug. 2023), available at: https://www.india-briefing.com/news/digital-india-bill-2023-key-provisions-stakeholder-perspectives-28755.html (last visited on July 3, 2025)
[28] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023*, available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited July 5, 2025).
[29] Digital India Portal, *MeitY's Dialogue on Digital India Bill and Stakeholder Engagement*, available at: https://www.digitalindia.gov.in (last visited on July 3, 2025).
[30] TCS, *FAQ on Proposed Digital India Act*, (2023), available at: https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/investor-relations/faq/proposed-digital-india-act.pdf (last visited on July 3, 2025).

Chapter V

Comparative Legal Frameworks

5.1 How other jurisdictions are tackling deepfakes:

Deepfakes are synthetic media generated using artificial intelligence that can alter audio, video, or images. They truly represent a threat to our privacy, democracy, and public trust. As deepfake technologies continue to proliferate across a variety of domains (including entertainment, politics, and misinformation), states across the globe are building out legal and regulatory frameworks to address the emerging harms from deepfakes. This will consider how different jurisdictions the United States, European Union, and China have begun to respond to the deepfake challenge and also identifies important equities for India to consider while shaping its own policy response.

5.1.1 United States

In the U.S., regulation of deepfakes occurs in a mixed way with federal and state proposals. At the federal level, the Deepfakes Accountability Act (2019/2023) is designed to criminalize non-consensual deepfake content created without consent. Additionally, the Take It Down Act (May 2025) requires online platforms to take down non-consensual intimate imagery created using AI, as well as other types of non-consensual intimate imagery, within 48 hours of receiving a notice of takedown.[31]Yet, there are First Amendment-related countervailing constitutional interests that allow for labels or censored satirical or political deepfakes.[32] At the state level, for example, California, Texas, Virginia, Minnesota, and Tennessee (e.g., TN's ELVIS Act), along with other partial organizations, have laws to address production regarding political deepfakes, revenge porn, and voice cloning. From these various state measures, we can see that most provide some sort of remedy focused on consent or removal of content but still allowing free speech, despite inconsistencies of application.

5.1.2 European Union

Europe has taken a more comprehensive approach and proactive approach. The EU has an AI

[31] Emily Miller, "Congress advances deepfake and revenge-porn law", *The Washington Post*, April 28, 2025.
[32] Lata Nott, *Deepfakes and the First Amendment*, (7 May 2025), *available at* https://www.freedomforum.org/deepfakes-protected-by-first-amendment (last visited 3 July 2025).

Act (coming into effect August 2024), in which AI applications including deepfakes are classified by risk where it requires transparency disclosures of general-purpose AI and requires that synthetic media is labeled. The Digital Services Act requires platforms to mitigate misinformation and manage systemic risk introduced with AI[33]. However, there is still ambiguity in definitions and how it will be enforced in practice definitional disputes abound over what a "deepfake" is, what constitutes "substantial editing," and how conflicting transparency obligations will apply in practice.[34] Nevertheless, the EU regulatory model is unique by its risk-based classification system, extraterritoriality, and harmonization across member states.

5.1.3 China

China has some of the strictest controls, with watermarking, identity verification, labeling (e.g. morse codes in audio), and banning misinformation and deception. The Deep Synthesis Provisions (January 2023) require consent from users, content traceability, data safety, and an audit of the algorithms. [35] There is strict enforcement of these rules by the Cyberspace Administration and they embody China's wider information control strategy to reinforce digital governance.

5.2 Lessons for India

By adopting a regulatory framework that is risk-based, transparent, and respects rights, India will be able to draw on global best practice. International examples show us that India should include consideration of consent mechanisms, mandatory watermarking, prompt takedown procedures, and platform responsibility. Chapter VII includes a detailed list of such recommendations that are made specifically with India's constitutional values and technology needs in mind.

[33] Claudia Koon Ghee Wee, *Artificial illusion: Global governance challenges of deepfake technology* (23 Apr. 2025)

[34] Kristof Meding & Christoph Sorge, *what constitutes a Deep Fake? The blurry line between legitimate processing and manipulation under the EU AI Act* (arXiv preprint, submitted 13 Dec 2024; rev. 4 Feb 2025)

[35] Michael Sumner, *Deepfake Disclosure Laws: Global Approaches 2024*, *available at* https://www.scoredetect.com/blog/posts/deepfake-disclosure-laws-global-approaches-2024 (last visited 3 July 2025).

5.3 Conclusion

The comparison shows that while the U.S., EU, and China have reached different views on a regulatory approach- consent, transparency, and traceability (even if not a uniform regulatory approach), India does not have an established unified legal method of responding to deepfakes. From these global models, there is considerable scope for India to do so and thereafter chart a path forward. In doing this, the next chapter highlights how courts and policymakers- up to now- have reacted in India, as well as showing in what areas there are shortcomings.

Chapter VI

Judicial and Policy Response in India

6.1 Role of Judiciary in Handling Misinformation

India's judiciary has played a dual role: reinforcing constitutional freedoms while recognizing evolving digital harms.

1. **Rajat Sharma & Anr. v. Tamara Doc & Ors. (Delhi HC)[36]**

In this landmark situation, seasoned journalist Rajat Sharma was able to seek an ex-part injunction from the Delhi High Court. This injunction was against eight defendants who made deepfake advertisement (promotional videos) of Sharma endorsing pharmaceutical drugs. Justice Amit Bansal noted that the use of Sharma's name, likeness, voice, and persona without consent, more so by way of "existing or future technology such as AI, deepfake technology", resulted in "irreparable harm" not only to his reputation, but also potentially damaging public health by misleading consumers. The Court also directed the online platforms, such as Meta, to take down this content and established a strong precedent on personality rights in the digital and AI era.

2. **Global Health Ltd. & Dr. Naresh Trehan v. John Doe & Ors. (Delhi HC)[37]**

[36] *Rajat Sharma & Anr. v. Tamara Doc & Ors., 2024 SCC Online Del 1578*
[37] *Global Health Ltd. & Dr. Naresh Trehan v. John Doe & Ors., 2025 SCC Online Del 2251*

In the same line of reasoning, the case also involved well-known medical professional Dr. Naresh Trehan, a heart surgeon, who had a deepfake video posted on social media that falsely appeared to endorse unverified and unproven methods to treat urological conditions. In that regard, the Delhi High Court granted a John Doe injunction that directed that intermediaries remove infringing content within a period of 24-36 hours, and to provide identifying information in relation to anonymous content creators. The case concerned not only a clear violation of personality rights, but also a public safety and security issue that could potentially mislead millions of people when an impostor can fraudulently represent a trusted professional in order to directly mislead the public.

3. Arijit Singh v. Codible Ventures & Ors.[38]

In a landmark decision, the Bombay High Court has recognized voice cloning as a breach of personality rights. In making its determination the Court established a three-pronged test: the plaintiff must be a celebrity, the cloned medium must identify the celebrity and the cloning must be in the name of commercial gain; the injunction also included an AI machine-generated voice and likeness across not just platforms but digital mediums, including the metaverse, advertisements and GIFs. This decision links the domain of deepfake technology to the domain of intellectual property, and provides a test for defining a legal boundary to the unauthorized activity of machine-generated AI remakes.

4. Shreya Singhal v. Union of India [39]

This case is a landmark case in online speech regulation because it struck down vague provisions under Section 66A of the IT Act, revisited intermediary liability pursuant to Section 79, protected free expression and made it imperative to obtain a court order to remove content. The legal principles provide a way to regulate deepfake contents without needlessly restraining freedom of speech but will also serve as a compass for future policy frameworks.

5. Justice K.S. Puttaswamy v. Union of India [40]

Although it does not specifically deal with the issue of deepfakes, this ground-breaking Supreme Court ruling establishing privacy as a basic right under Articles 14, 19, and 21 has

[38] *Arijit Singh v. Codible Ventures, 2024 SCC Online Bom 1205.*
[39] *Shreya Singhal v. Union of India, (2015) 5 SCC 1 (SC).*
[40] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (SC).

paved the way for subsequent litigation in the AI/digital space. It requires that any breach into personal autonomy, including impersonation through a deepfake and the creation of content without consent, must pass tests of legality, necessity, and proportionality, making it an important legal precedent against digital manipulation.

6.2 Government Advisories or Committee Reports

Government Advisories & Reports on Deepfakes and Misinformation

1. Ministry of Electronics and Information Technology (MeitY)

- MeitY's Guidelines and Action on Misinformation o MeitY has released several advisories on misinformation, with a particular focus on social media.
- They focus on things such as taking down content, engaging with the platforms, and running public awareness campaigns.
- Although the deepfake content is not always mentioned explicitly, their general misinformation framework does include synthetic media.[41].

2. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

- These regulations obligate social media intermediaries to keep a check over misinformation and regulate it.
- Platforms must have grievance redressal mechanisms and remove illegal content without delay, including fake videos/deepfakes.
- It is one of the most robust regulatory frameworks to unquestionably tackle digital misinformation.[42]

[41] Ministry of Electronics and Information Technology, Government of India, *Available at:* https://www.meity.gov.in *(last visited July 3, 2025).*

[42] Ministry of Electronics and Information Technology, *Intermediary Guidelines and Digital Media Ethics Code Rules* (1st edn, Government of India, New Delhi, 2021) (Last date visited on 3 July 2025)

3. Parliamentary Standing Committee on Information Technology

- Have also examined from time-to-time, the challenges presented by fake news and misinformation.
- They have included explanations in their reports of the most recent threat of AI-based synthetic content and encouraged tighter regulations and awareness campaigns.
- These discussions even offer the idea of applying technology to detect deepfakes.[43]

4. Election Commission of India (ECI)

- The ECI actively works to combat misinformation and fake news during elections.
- Issued advisories about false information on social media affecting the electoral process.
- Has started to incorporate AI tools and fact-checking partnerships to detect deepfake videos and other misleading content during elections.[44]

5. NITI Aayog

- In discussions about the ethics of Artificial Intelligence NITI Aayog has acknowledged the potential risk that indeed AI can be misapplied in the generation of deep fakes and initiates misinformation.
- To that end, it recommends fostering AI research - including detection of synthetic content - and regulation.[45]

6. Cyber Crime Cells and CERT-In

- Alerts were put out by the Indian Computer Emergency Response Team related to cyber

[43] Lok Sabha Secretariat, *Report No. 26 of the Standing Committee on Communications and Information Technology on Suspension of Telecom/Internet Services and Its Impact*, 17th Lok Sabha, Government of India, New Delhi (2021)
[44] Election Commission of India, *Advisory on AI and Deepfake Content for Political Parties*, Government of India, New Delhi (6 May 2024)
[45] NITI Aayog, *Approach Document on Responsible Artificial Intelligence*, Government of India, New Delhi (2023)

threats, some of which are misinformation campaigns leveraging AI.

- Several cybercrime units throughout the states are receiving increasing training on how to process complaints involving deepfake videos or fake digital content.[46]

Other Initiatives:

- Fact-checking networks and collaborations supported by the government and NGOs to combat misinformation

- Campaigns on awareness of digital literacy, including helping citizens to identify fake content.

Some startups and research institutions in India are building deepfake detection tools, often using government funding.

6.3. Ethical Concerns and Human Rights Implications

The ethical issues connected to deepfake technology with respect to privacy, human dignity, and free speech have been contemplated conceptually in Chapter II. These values have emerged as judicially cognized within India through a growing development of personality rights jurisprudence in India, which includes the more recent decisions of **Amitabh Bachchan v. Rajat Negi** and **Arijit Singh v. Codible Ventures**. Not only have the courts acknowledged reputational harms, but also breaches with respect to digital identity. The recent developments from the courts reiterate an ethical argument for the need for legal reform.

For instance, in **Amitabh Bachchan v. Rajat Negi**, the Delhi High Court contended that un-authorised likenesses generated through AI were breaches of personality rights and privacy. Similarly, in **Arijit Singh v. Codible Ventures,** the Bombay High Court found that the cloning of a celebrity's voice contravened digital dignity.

However, these are all case specific responses. Mid level solutions are needed, which take into consideration the issues related to abuse of power and over criminalization, and having a balance between freedom of speech and preventing harm. An ethical framework needs to be

[46] Indian Computer Emergency Response Team (CERT-IN), *Homepage*, Ministry of Electronics and Information Technology, Government of India, available at https://cert-in.org.in/ (Last date visited on 3 July 2025)

articulated, reflecting the ethical framework that needs to be codified into law in India and adopted by the digital ecosystem.

6.4 Empirical Trends and Visual Representation

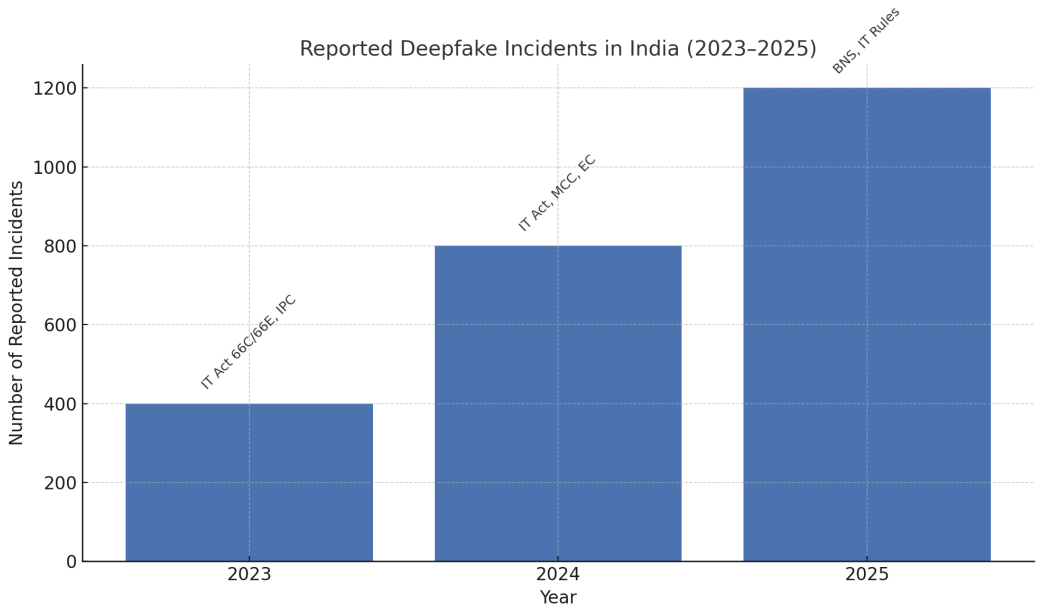

Figure 1: Increase in Reported Deepfake Incidents in India (2023-2025) Aggregated data based on alerts from the Indian Computer Emergency Response Team (CERT-In), advisories from the Ministry of Electronics and Information Technology (MeitY), media reports, and parliamentary reports on AI-generated disinformation and takedown notices. Legal action changed from armed enforcement under the IPC and IT Act in 2023, to enforcement via BSN 2023 and drives for digital governance.

Based on empirical data and trends, there has been a sharp increase in incidents involving 'deepfake', or AI-manipulated video-based incidents in India. With total numbers of incidents derived from the CERT-In database, MeitY advisories, and Election-related takedown notices, it is estimated that India had just less than 400 reports of deepfake incidents in 2023, escalating to an estimated 800 incidences in 2024, to estimates that could go as high as 1200 incidences by the end of 2025. This growth represents both the advancements in AI tooling, along with the growth of synthetic content across the social landscape.

As given above graph demonstrates, the evolution of the legal and regulatory responses have shifted from gradual implementation of the existing provisions under the Information

Technology Act, 2000 and Indian Penal Code in 2023, to preliminary directives from the Election Commission and implementation of the Model Code of Conduct as of 2024, to the latest use of the Bharatiya Nyaya Sanhita (BNS) 2023, proposed Digital India Bill, and interim updated intermediary guidelines in 2025.[47]

This empirical journey gives strong justification to the paper's principal finding: India must move from reactive, fragmented enforcement to a systematic, anticipatory regulatory regime underpinned by the use of watermarking, algorithmic audits, accountability via platforms, and civic media literacy as fundamental principles for the governance of the AI era.

6.5 Conclusion

India's judiciary and government have taken important steps to address deepfakes through injunctions, advisories, and policy discussions, yet these responses remain largely reactive and case-specific. Despite growing legal recognition of personality rights and digital harms, the absence of a unified legal framework limits consistent enforcement. This calls for a forward-looking strategy, which the next chapter outlines through key recommendations for a comprehensive and anticipatory legal and policy response.

Chapter VII:

Recommendations and the conclusion

7.1 Recommendations

To effectively address the growing threat posed by deepfakes in India, this paper proposes a multi-pronged strategy combining legal, institutional, technological, and educational reforms.

7.1.1 Legal and Regulatory Reforms

1. **Enact a Standalone Deepfake Regulation Act**

- Introduce a stand-alone definition of "synthetic media" and "deepfake" as legal terms

[47] Indian Computer Emergency Response Team (CERT-In), Annual Cybersecurity Reports (2023–2025); MeitY, Advisory on Deepfake Metadata (Mar. 2024); Press Trust of India, "Govt's Advisory to Social Media on Deepfake Rules", Business Standard (Dec. 26, 2023); The Hindu, "EC Warns Political Parties Against AI Misuse" (June 28, 2024); The Times of India, "Navsari Man Held for Sharing Deepfake Video of PM" (May 16, 2025).

in a new statute.

- Establish criminal (or civil) penalties for malicious creation, dissemination, or transmission of deepfakes without consent

2. Amend Existing Cyber Laws

- Amend the Information Technology Act, 2000, or add provisions for deepfakes in the upcoming Digital India Bill.

- Sections 66C, 66E and 67A should be amended to include AI-generated impersonation and unauthorized synthetic content.

3. Statutory Recognition of Personality and Digital Rights

- Recognize and codify digital personality rights under Indian law to prevent unauthorized use to replicate likeness, voice, and visual identity by AI.

- Require that these rights recognized as extending Article 21 of the Constitution.

7.1.2 Institutional and Platform-Level Accountability

1. Mandatory Watermarking and Metadata Disclosure

- Require platforms and developers of AI to always embed watermarks or origin metadata into any content produced by AI.

2. Strict Takedown and Reporting Regime

- Change the intermediary guidelines to enforce the removal of flagged deepfake content to 24 hours.

- Require transparency reports on the number of takedown requests and action taken.

3. Establish a Deepfake Regulatory Task Force

- Create a separate unit within CERT-In or MeitY to investigate and respond to complaints of cyber matters related to deepfakes.

- Give the Election Commission the power to issue takedown orders during an election period without going to court first

7.1.3 Judicial Oversight and Rights-Based Framework

1**. Adopt the Puttaswamy Test for Detection Mechanisms**

- Have any deepfake detection mechanism that is implemented or sponsored by the state satisfy legality, necessity and proportionality under the Puttaswamy judgment.

7.1.4 Public Education and Digital Literacy

1. **Media Literacy Campaigns**

- Implement nationwide public awareness campaigns aimed at informing citizens about the existence, risks, and detection of deepfakes.

2. **Digital Ethics in Education**

- Embed education modules on artificial intelligence (AI) ethics, media misinformation, and critical thinking with digital engagement in secondary and post-secondary education curricula.

7.2 Conclusion

This research demonstrates that while India's legal system and judiciary have begun to confront the harms of synthetic media, their responses have been hit or miss. Existing privacy and personality rights protect situations but lack statutory authority for consistent enforcement.

Borrowing from the world's experience, India should establish a forward-thinking, multi-level regulatory framework to balance future innovation with fundamental constitutional rights in Articles 19(1)(a), 19(2), and 21. Deepfakes regulation should incorporate the broader interpretations of national security and election manipulation, and include deepfakes regulation of harms, including issues of digital dignity, informational autonomy, and protection of citizens from information and communication harms.

To this end, India should:

- Establish targeted legislation specific to the definition of deepfake, and the implications of creating or dealing in deep fake content.

- Mandate disclosure, watermarking, and traceability requirements for media created by an AI.

- Prioritize intermediary liability under statutory timelines for platforms.

- Establish national digital literacy programs and awareness programs to build user power.

It is not enough for legal development to happen in statutes, but in regulatory philosophy and ultimately regulatory preparedness. Without change, the unmade scaffold surrounding deepfakes will continue to undermine public trust, democratic future, and the rule of law.

BIBLIOGRAPHY

Primary Sources

Statutes

1. The Constitution of India, Article 19(1)(a), read with Article 19(2).
2. The Information Technology Act, 2000.
3. The Bharatiya Nyaya Sanhita, 2023 (India).
4. The Copyright Act, 1957, Act No. 14 of 1957.

Case Laws

1. Rajat Sharma & Anr. v. Tamara Doc & Ors., 2024 SCC Online Del 1578.
2. Global Health Ltd. & Dr. Naresh Trehan v. John Doe & Ors., 2025 SCC Online Del 2251.
3. Arijit Singh v. Codible Ventures & Ors., 2024 SCC Online Bom 1205.
4. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (SC).
5. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (SC).
6. Amitabh Bachchan v. Rajat Negi, 2022 SCC Online Del 3625.
7. Anil Kapoor v. Simply Life India & Ors., 2023 SCC Online Del 4532.

Secondary Sources

Journal Articles

1. Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107(6) California Law Review 1753.
2. Jan Kietzmann, Ian P McCarthy and Leyland Pitt, "Deepfakes: Trick or Treat?" (2020)

63(2) Business Horizons 135.

3. David MJ Lazer et al., "The Science of Fake News" (2018) 359(6380) Science 1094.

4. Cristian Vaccari and Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News" (2020) 6(1) social media + Society.

5. Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making" (2017) Council of Europe.

6. Tobias Dobber et al., "Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?" (2021) 26(1) The International Journal of Press/Politics 69.

Government Websites

1. Ministry of Electronics and Information Technology, Government of India, https://www.meity.gov.in (last visited 3 July 2025).

2. Election Commission of India, Official Website, https://eci.gov.in (last visited 3 July 2025).

3. NITI Aayog, Official Website, https://www.niti.gov.in (last visited 3 July 2025).

4. Indian Computer Emergency Response Team (CERT-IN), https://cert-in.org.in (last visited 3 July 2025).

5. Internet and Mobile Association of India, "Digital in India Report 2023", https://www.iamai.in (last visited 3 July 2025).

6. Telecom Regulatory Authority of India, "Monthly Performance Report for Internet & Broadband 2023", https://trai.gov.in (last visited 3 July 2025).

Government Reports

1. Ministry of Electronics and Information Technology, Intermediary Guidelines and

Digital Media Ethics Code Rules, 1st edn (Government of India, New Delhi, 2021).

2. Lok Sabha Secretariat, Report No. 26 of the Standing Committee on Communications and Information Technology on Suspension of Telecom/Internet Services and Its Impact, 17th Lok Sabha (2021).

Newspapers

1. The Hindu Bureau, "EC warns political parties against misuse of AI-based tools", The Hindu (New Delhi, 28 June 2024).

2. Priyali Prakash, "Explained | Highlights of the Proposed Digital India Act, 2023", The Hindu (18 March 2023).

3. Press Trust of India, "Govt's advisory to social media portals on IT rules over deepfake concerns", Business Standard (26 December 2023).

4. Deeksha Bhardwaj, "Draft of Digital India Bill to be Ready by First Week of June: Rajeev Chandrasekhar", Hindustan Times (24 May 2023).

5. Ishaan Tharoor, "India sieves online deluge, to stamp out disinformation in world's biggest election", Reuters (25 April 2024).

6. Emily Miller, "Congress Advances Deepfake and Revenge Porn Law", The Washington Post (28 April 2025).

Web Articles

1. Tucker P, "Deepfakes and the New Disinformation War", Defense One (18 January 2019),https://www.defenseone.com/technology/2019/01/deepfakes-and-new-disinformation-war/154002/ (last visited 3 July 2025).

2. Michael Sumner, "Deepfake Disclosure Laws: Global Approaches 2024", Scoredetect Blog (2024) https://www.scoredetect.com/blog/posts/deepfake-disclosure-laws-global-approaches-2024 (last visited 3 July 2025).

3. Ministry of Electronics and Information Technology, "Advisory on Misinformation and

Deepfake Mandating Unique Metadata", SCC Online Blog (7 March 2024) https://www.scconline.com/blog/post/2024/03/07/meity-issues-advisory-on-misinformation-and-deepfake-legal-news (last visited 3 July 2025).

4. Lata Nott, "Deepfakes and the First Amendment", Freedom Forum (7 May 2025) https://www.freedomforum.org/deepfakes-protected-by-first-amendment (last visited 3 July 2025).