LEGAL EVOLUTION IN THE AGE OF AI AND DATA PRIVACY

Babhravi Singh, Symbiosis Law School, Noida

ABSTRACT

In today's ever-evolving world of technology, the emergence of Artificial Intelligence (AI), deep learning, and algorithmic decision-making is transforming how societies operate. While these developments have tremendous advantages, they also create unique legal, ethical, and regulatory risks. Our current legal systems, the majority of which were developed when such technologies were not even a concept, are struggling to grow at a pace alongside the challenges of modern digital threats. When India's underlying digital laws were drafted, no one could have foreseen crimes such as AI-created deepfakes, scams based on voice cloning, or automated disinformation campaigns. The result is that legal frameworks integral to digital governance are beginning to fray and become obsolete.

The Information Technology Act of 2000 is foundational but out of date. The Digital Personal Data Protection Act 2023 was a step in the right direction, but technologies are growing faster than the legislation can be updated. India has released the Draft DPDP 2025 Rules for public draft consultation to accommodate this, which seeks to construct a more dynamic and adaptable legal framework for a changing digital environment.

This research takes a comparative doctrinal approach supported by a short primary survey measuring India's current and proposed digital legal frameworks against globally recognised analogs like the GDPR and the EU Artificial Intelligence Act. It also involves the Directive Principles of State Policy (DPSPs), accepting them as the constitutional baseline for future tech legislation. This research hopes to recommend revisions to the laws that effectively balance the drive for technological progress with the protection of rights. The research is cognizant of emerging AI-fuelled offences that current regulations do not adequately prohibit or punish. It proposes to add value to the discussion and raise suggestions to resolve the global issue of digital law in India by providing legal proposals from countries worldwide.

INTRODUCTION

As AI technologies develop at an incredible pace, India is struggling with the regulatory blind spots, more so in responding to harms caused by AI-generated synthetic media such as deepfakes and voice clones. ***While international peers have started developing express legal protections against synthetic media, India's current laws are wide, reactive, and technologically stale.*** This article questions how India's legal system is presently incapable of coping with the impending threats emanating from generative AI, especially in the guise of deepfakes and AI-voice clones. Though the technologies are still developing and embedding themselves into mundane online interactions, their abuse, spanning impersonation to disinformation, has gotten ahead of the legal protection. Instead of criticizing AI as a piece of technology, this research focuses on the prevailing statutory and rule-making frameworks, e.g., the Digital Personal Data Protection (DPDP) Act, 2023, and the Information Technology Rules, 2021, that are technologically lagging and have no express provisions to regulate synthetic media harms. Through doctrinal analysis and comparative intelligence from global legal prototypes, the paper illustrates how Indian law, though recognizing risk through judicial decrees and ministerial advisories, has still not developed into a cohesive, enforceable framework for AI-based deception. Whether the solution is in a single law or through codifying and modifying ones in place is in question,but the increasingly wide gap between legal blueprint and AI realities necessitates serious contemplation.

Learning from international legal frameworks in the EU, China, and U.S., the paper questions whether India needs an independent legislative regimen to govern synthetic media, or whether selective amendments to current legislation would be adequate. Although an absolute answer remains contingent upon emerging policy agendas, the analysis attempts to provide a frame for examination of rights-oriented, enforceable, and context-specific regulatory responses in the Indian digital ecosystem.

RESEARCH PROBLEM

With the growing abuse of deepfake and voice cloning technology, India still does not have a binding legislation that clearly defines, limits, or criminalises such artificial content. Though some of the malicious consequences of such technology, like financial fraud, obscenity, or defamation, are criminalised under various legislations, no legislation recognises the production or transmission of artificial media as an offence per se. This response strategy has the inadequacy

of failing to treat the root problem: people remain unprotected until harm is done, and enforcement measures prove ineffective in stemming the flow or spread of such material before damage has ensued. Lacking the proactive statutory protection, the law is mute at the time when intervention is most critical, before the harm.

RESEARCH OBJECTIVES

1. To identify the legal vacuums in Indian legislation regarding AI impersonation.

2. To analyze the Indian legislation with international standards.

3. To recommend legal and policy reform for the regulation of the research problem.

RESEARCH METHODOLOGY

This research follows a doctrinal legal research approach, where secondary reliance is placed mainly on analysis of statute texts, rules, and regulations like the Digital Personal Data Protection Act, 2023, and the Information Technology Act, 2000, as well as the IT Rules, 2021. Secondary sources like ministerial statements, judicial rulings, government notices, and policy reports are also analyzed in the paper. To place India's gaps in legislation in context, a comparative legal analysis is made with reference to international frameworks like the EU AI Act, China's Deep Synthesis Rules, and U.S. state legislation on synthetic media. This allows for assessing India's gaps in legislation against global legislative responses in evolution.

THE LEGAL BACKGROUND

The digital legal world in India commenced with the enactment of the Information Technology Act, 2000[1] (*hereinafter IT Act*), legislation that attempted to legally acknowledge e-commerce, digital signatures, and contracts through the internet. It was enacted when the internet was still a new tool, employed mostly for email and static web surfing. ***The IT Act addressed the then prevailing needs: cyber fraud, simple hacking, obscenity, and identity theft.***[2] Subsequent amendments were made, adding offences such as cyber terrorism (Section 66F[3]), and breaches of data privacy (Section 72A[4]It was soon realized that the law had become technologically

[1] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[2] PAVAN DUGGAL, CYBERLAW: THE INDIAN PERSPECTIVE (2d ed., Universal Law Publishing 2010).
[3] Information Technology Act, 2000, § 66F, No. 21, Acts of Parliament, 2000 (India).
[4] Information Technology Act, 2000, § 72A, No. 21, Acts of Parliament, 2000 (India).

outdated in the era of mobile apps, data spying, and AI-based ecosystems.

Section 72A of the IT Act, for example, criminalizes disclosure of personal data by a service provider in contravention of a contractual terms, without addressing situations where data is collected by artificial intelligence with no contractual arrangement, e.g., virtual assistants (like Siri or Alexa) always recording voice data, or apps scraping users' location and biometric patterns in real time. ***The statute does not mention any provision that criminalises the hidden profiling of individuals by AI-powered algorithms.*** The Act also fails to take into consideration third-party misuse of data enabled through AI-powered tools such as deepfakes and voice cloning, which are currently weaponised in financial fraud, impersonation, and political misinformation.[5]

In response to growing concerns about data security, algorithmic profiling, and consent-based processing, the Indian legislature passed the Digital Personal Data Protection Act, 2023[6] (hereinafter DPDP Act). This act introduced the new-era legal constructs like data principal, data fiduciary, notice and consent, and proposed the idea for the creation of the Data Protection Board of India.[7] It signaled a shift from a punitive model towards civil liability, aligning India's regulatory approach more closely with international norms, notably the European Union's General Data Protection Regulation (GDPR).[8]

1.1 Insufficient India's Legislation in New Era

Even with India's recent legislative forays, the Digital Personal Data Protection (DPDP) Act, 2023, and Information Technology (IT) Act, 2000, have no specific provisions to manage synthetic content created by AI systems. For example, Section 6[9] of the DPDP Act, providing for withdrawal of consent, ceases to apply once data has been utilized to train AI models, illuminating a theoretical control vs. practical irreversibility gap. Section 8(2)[10] enforces data minimization, but AI technology regularly captures over-the-top datasets to train on without substantial oversight. Section 9[11] (security measures) does not enforce watermarking, labelling,

[5] Internet Freedom Foundation, India's Deepfake Threat: Why Current Laws Are Not Enough (2023), https://internetfreedom.in.
[6] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[7] Id.
[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[9] Digital Personal Data Protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).
[10] Digital Personal Data Protection Act, 2023, § 8(2), No. 22, Acts of Parliament, 2023 (India).
[11] Digital Personal Data Protection Act, 2023, § 9, No. 22, Acts of Parliament, 2023 (India).

or any AI-oriented transparency measures. The IT Act, on the other hand, criminalizes offensive material under Section 66E[12] (violation of privacy), Section 66D[13] (personation), and Section 67[14] (obscenity), but none of these sections tackle deepfakes at the time of their creation and none criminalize personation through AI unless other offenses are caused. In addition, Section 79[15] gives intermediaries safe harbor, restricting liability even when platforms have AI-generated disinformation present. These legislations together counteract downstream impacts but do not touch upon the production, training, or distribution of fake AI content, making them obsolescent in the era of current generative technologies.

1.2 The DPDP Act does so only partly in dealing with the actual harms of the digital era

i. It lacks a mandatory timeline, as in contrast to GDPR's 72-hour requirement, Indian businesses are not obligated to inform users about data breaches within a specific time frame.

ii. It just governs digital personal data, excluding issues of non-personal data and synthetically created content such as deepfakes and AI-created impersonations.

iii. It doesn't place strict obligations on platforms such as YouTube or Meta to remove doctored material that infringes on a person's dignity or identity.

A major paucity of the Act is that it fails to regulate the use of anonymised or publicly accessible data, forms of data that are often used to train artificial intelligence models without the consent or knowledge of the data subject. As the legislation does not consider such data as personal data, its exploitation remains unregulated, thus creating a large legal gap. This omission enables AI developers to bypass consent and accountability mechanisms, raising grave concerns regarding data autonomy and user protection.

This legal vacuum becomes even more concerning in light of real-world incidents. For example, in the case of ***Ankur Warikoo's deepfake fraud***[16], his face and voice were artificially mimicked to market fake investment schemes. The respite was in the form of a ***John Doe injunction*** by the court under the IT Act , an ex parte limited civil remedy that granted temporary blocking or takedown of the material. This is not to say the IT Act is exhaustive or capable of dealing with

[12] Information Technology Act, 2000, § 66E, No. 21, Acts of Parliament, 2000 (India).
[13] Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).
[14] Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).
[15] Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).
[16] *Ankur Warikoo and Anr v John Doe and Ors* (Delhi HC, 26 May 2025)

deepfake-based offenses. It has no clear provisions criminalizing AI-fabricated impersonation, with victims only receiving procedural relief and not substantive protection. The DPDP Act, 2023, does not provide any assistance here, as it provides no enforceable remedy for abuse of publicly available or non-consensually obtained personal data. Collectively, these loopholes reveal a grave legal vacuum within India's regulatory landscape, especially in light of fast-developing AI technologies.[17]

These constraints spurred the issuance of the Draft DPDP Rules in January 2025[18], which are now subject to public consultation. The draft brings new categories such as "significant data fiduciary", prescribes data retention and child protection obligations, and attempts to provide for procedures for the withdrawal of consent and grievance redressal. Yet even these Rules fail to cover the threats that arise from automated observation, deep-fake content, or AI impersonation technology such as voice clones that have already been used in financial fraud and political blackmail crimes.

These legislations fall short in governing AI-facilitated manipulation, impersonation in digital space, and non-consensual data creation. This article aims to analyze how India's existing and pending legal regimes may be reformed, learning from international models such as the GDPR.[19] and the EU AI Act[20] , to safeguard constitutional values, innovation, and the digital dignity of citizens in an algorithmic world.

2. LEGAL LACUNAE IN INDIA'S AI LEGISLATION

2.1 The Consent Dilemma: Informed or Imposed?

Even though the DPDP Act, 2023, mandates data fiduciaries to seek the consent of the data principal prior to processing personal data, consent is often neither free nor informed.[21] Increasing numbers of mobile apps, websites, and digital services utilize bundled consent practices, where declining permission leads to a total denial of service. Users are regularly

[17] Bharvi Shahi & Anand Raj Dev, Navigating India's Digital Personal Data Protection Act: Critical Implications and Emerging Challenges, 3(1) INT'L J. L. SOC. SCI. STUD. 42 (2024).
[18] Draft Digital Personal Data Protection Rules 2025 (Ministry of Electronics and Information Technology, Government of India, 5 January 2025) accessed 2 July 2025
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[20] Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, 2024 O.J. (L 1689) 1 (Artificial Intelligence Act).
[21] Sara Quach et al., Digital Technologies: Tensions in Privacy and Data, 50 J. ACAD. MARKETING SCI. 1299 (2022).

compelled to accept sweeping data-sharing provisions, microphone, camera, storage, contact list, or real-time location access, in exchange for access to apps that are essentially necessary.[22]

The generic argument of digital platforms is that one has the liberty to opt out and not use the service. But this collapses in real life, where some of the most important digital platforms are integral to everyday life. UPI apps like Phone Pe or Google Pay are now an integral part of fundamental payments. Students can't do without school apps, employees get onboarded through HR technology platforms, and job seekers turn to LinkedIn. Government services such as CoWIN, Digi Locker, and Aarogya Setu have gone digital-first for public services. Such functional reliance denies people actual choice, making consent more of an illusion than a legal protection.

While India lacks a clear legal norm for defining what constitutes "free consent" in online settings, global standards like Recital 43[23] the GDPR establishes that consent cannot be valid if it is made dependent on services that are not essential and for which the data being collected is not necessary. Put differently, making users provide non-obligatory personal information as a prerequisite to receiving a service is not permitted according to global standards.

Indian law, and notably in the case of ***Justice K.S. Puttaswamy v. Union of India***[24], has recognized that informational privacy rights include protection against State as well as private actors. The DPDP Act, 2023, falls short in turning these principles of privacy into binding obligations. As a result of this, there is still a gap between the acknowledgment of privacy rights and the extent of legal protection individuals enjoy in cyberspace.

The inability to undo or reverse the harm caused by AI or trained AI content poses a serious challenge to the provision of consent in the current legislation; these practical gaps are discussed further in the following section.[25]

2.2 Consent Beyond Recall: Regulatory Challenges in AI Learning

The DPDP Act details a grievance redressal mechanism under Section 13[26], where data

[22] D.P. MITTAL, COMMENTARY ON THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (Commercial Law Publishers 2024).
[23] Regulation (EU) 2016/679, recital 43.
[24] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[25] Giada Pistilli and Bruna Trevelin, 'Can AI be Consentful?' (2025, preprint, Cambridge University Press chapter, arXiv) accessed 16 July 2025.
[26] Digital Personal Data Protection Act, 2023, § 13, No. 22, Acts of Parliament, 2023 (India).

fiduciaries or consent managers are mandated to resolve complaints prior to the individual resorting to the Data Protection Board. Yet when it comes to AI-driven harms, this grievance redressal mechanism breaks down on both technical and practical fronts, rendering it ineffective in offering real remedies. AI systems that are trained on personal information, such as voice snippets, images, or user activity, don't keep that information in a manner that can be traced or deleted later.[27] If your data is used to train an AI model, then it becomes part of what the system does. ***So even if you withdraw your consent later under Section 6[28] of the DPDP Act, that does not erase your data from the model nor reverse what the AI has learnt already.*** At present, there is no legislation that forces firms to remove your information from AI systems or retrain their models when you withdraw consent.[29] The danger presented by artificial intelligence technologies goes beyond issues of legality to accessibility and abuse.[30]

There have been cases where individuals have been tricked into sending money after receiving fake calls in the voice of a family member, or swayed by AI-written political speeches designed to influence voting patterns.[31] The victims are intimidated or extorted through explicit synthetic materials generated by third parties without consent or knowledge, with the help of AI. Such activity not only amounts to cyber deception but also causes psychological harm, economic loss, and the dissemination of misinformation, all of which continue to be impossible to trace, monitor, or prosecute under India's current legal framework.[32]

Even in situations where redress of grievances is pursued, enforcement is practically impossible. A deepfake shared on various platforms or a voice clone utilized for fraud can be replicated, downloaded, and shared over and over again, and is unlikely to be taken down.[33] No such centralized AI redressal system exists through the law, watermarking requirements, or live content moderation equipment like the EU Digital Services Act. Automated platforms such as chatbots or voice assistants usually do not qualify as Indian data fiduciaries, and might not offer any recourse for complaints by users, thus further diluting protections. As injuries are caused in real time and the data runs amok, India's current paradigm has no effective pre-emptive or post-

[27] Lauren Leffer, Your Personal Information Is Probably Being Used to Train Generative AI Models, SCIENTIFIC AMERICAN (Oct. 19, 2023), https://www.scientificamerican.com.
[28] Digital Personal Data Protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).
[29] Leffer, *supra* note 27.
[30] A. Feder Cooper et al., Machine Unlearning Doesn't Do What You Think: Lessons for Generative AI Policy, Research, and Practice (2024).
[31] Id.
[32] Anni Coonan, 'Audio and Video Deepfakes: A Cutting-Edge Scam and Disinformation Risk' (Steptoe & Johnson, 20 October 2024) accessed 6 July 2025
[33] Leffer, *supra* note 27.

incident recourse.[34]

The lack of enforcement infrastructure is but half the issue. The more profound issue is the law's silence on the very essence of AI-generated falsehood. Even where platforms refuse to take down problematic synthetic material, the law provides no remedy unless that material leads to a standalone offence for which they can be prosecuted.[35] This lacuna, where creation and dissemination of deepfakes or voice clones are not offenses in themselves, gives such technology room to be properly untrammelled. The subsequent section reveals how this lacuna leaves perpetrators free from accountability, even when victims suffer real and often irreparable damage.

2.3 Legal Silence Before the Harm: India's Failure in Pre-emptive AI Safeguards

Though India criminalises certain effects of data abuse, i.e., cheating (Section 318(4) of BNS, 2023[36]), defamation (Section 356 of BNS, 2023[37]), or dissemination of obscene content (Section 67 IT Act[38]), no express prohibition exists on the production or dissemination of deepfakes or voice clones in and of themselves. Such omission renders these harms legally nameless. To illustrate, in many recent voice phishing cases, like the 2024 Mumbai case, where AI-generated emergency calls impersonated family members, the accused were prosecuted for financial fraud and not for the synthetic impersonation per se. Likewise, in Hyderabad, deepfake pornography created through public social media photographs resulted in action under obscenity laws, but the creation of the deepfake video was not criminalized in its own right. Section 6[39] of the DPDP Act permits the use of publicly available data without consent. ***Thus, it is legally permissible to web scrape an individual's public images, voice clips, or videos to train AI models.[40] No law explicitly defines "synthetic content,"[41] criminalizes AI-enabled impersonation, or prescribes takedown processes for the same material.*** Consequently, these harmful AI-generated content

[34] H Akin Ünver, *Artificial Intelligence (AI) and Human Rights: Using AI as a Weapon of Repression and Its Impact on Human Rights* (Policy Department for External Policies, European Parliament, May 2024) PE 754.450 accessed 10 July 2025
[35] Charlotte Stanton, Thomas E Kadri, David Danks, Jack Parker and Megan Metzger, *The Legal, Ethical, and Efficacy Dimensions of Managing Synthetic and Manipulated Media* (Carnegie Endowment for International Peace, 15 November 2019) accessed on 2july, 2025
[36] Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).
[37] Bharatiya Nyaya Sanhita, 2023, § 318(4), No. 45, Acts of Parliament, 2023 (India).
[38] Bharatiya Nyaya Sanhita, 2023, § 356, No. 45, Acts of Parliament, 2023 (India).
[39] Digital Personal Data Protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).
[40] Id.
[41] Lawrence Hurley, Managing Reputation in the Age of Synthetic Content, REUTERS (July 18, 2025), https://www.reuters.com.

functions operate unregulated, shielded from liability unless their conduct violates another specific law.

In other parts of the world, jurisdictions such as the EU under its Artificial Intelligence Act and the U.S. under forthcoming state laws (such as California's deepfake election law[42]) are now starting to distinguish between synthetic media, mandate watermarking or disclosure requirements, and criminalize impersonation using AI. ***However, India has no legislative lexicon to identify these harms as distinct.***

Unless confronted, the dangers will only grow: election manipulation, court tampering, economic fraud, psychological damage, and lack of belief in audio-visual proof. The criminal justice system, founded upon human witnesses and material truth, will find it hard to respond in an age when artificial falsehoods can be as hard to distinguish from actual speech and action.

Collectively, these loopholes unveil a perilously deficient legal code that cannot keep pace with the needs of the AI age. Consent structures[43] Under the DPDP Act, grievance redressal mechanisms is superficial, it is ineffective in AI settings, and even the activity of creating synthetic content is still outside the purview of criminal law. This piecemeal strategy constrains accountability and renders victims bereft of real redress in the event of actual harm. As more technologies develop at a pace ahead of regulation, such legal voids must be plugged by focused reform, strong protections, and statutory identification of AI-independent dangers, questions to which the subsequent sections seek to delve in comparative and constitutional terms.[44]

2.4 Beyond Illusion

Deepfakes are the equivalent of an exploding ticking time bomb. The DSCI Exploratory Note highlights how these AI-generated forgeries undermine trust in its foundation, trampling privacy, weaponizing identities, and disrupting democratic conversation.[45] In India, the legal void is stark: there is no definition of "synthetic content," no criminalization of its manufacture, and no watermarking or traceability requirement to stem its viral transmission.[46] In the meantime, other countries have stepped up, China's Deep Synthesis Rules, California's deepfake election law,

[42] California Assembly Bill 2355 (Political Advertisements: Artificial Intelligence) (2024)
[43] Regulation (EU) 2016/679, art. 4(11).
[44] Giada Pistilli and Bruna Trevelin, 'Can AI Be Consentful?' (2025, preprint, Cambridge University Press chapter, arXiv) accessed 22 July 2025
[45] Data Security Council of India, Exploratory Note on Deepfakes (2023).
[46] Id.

and Article 52[47] of the EU AI Act already place proactive obligations. The Note cautions that waiting for reactive takedowns or consent-based safeguards is useless when deepfakes can ruin reputations, sway elections, or spark riots before the truth arrives. India cannot do piecemeal; it has to create a future-proof legal response that gives deepfake producers pause before they click "generate."[48]

3. THE UNADDRESSED DANGERS

Today's society is confronted with a tidal wave of synthetic offenses that were unimaginable a decade ago. Deepfakes and voice cloning tools, once the preserve of research experiments, are now readily available, intuitive, and rapidly weaponised for use by criminals. They create significant challenges to privacy, dignity, democratic stability, and financial security. However, India's legal system still has no specific recognition or regulation of such content.

3.1 From Technology to Threat: The Rise of Deepfake and Voice Clone Crimes

Several high-profile cases in India highlight the seriousness of the matter:

- **Mumbai Voice Clone UPI Scam (2024):** In the incident, scammers employed publicly known voice samples to clone a woman's relative and fabricated an urgency to prompt her to send money via UPI. Though the accused were registered for cheating, there was no responsibility for generating or utilizing a synthetic voice impersonation.

- **Political Disinformation through Deepfake[49] (Delhi, 2023):** A video of a high-profile political leader spewing inflammatory rhetoric, generated using AI, went viral one day before municipal elections. The video turned out to be fake later, but no action was taken against those who made it since no law penalised the creation of artificial political content unless it led to rioting or some other cognisable offence.

  This shows that AI-generated deception is increasing, yet legal instruments are lagging behind. Harm is only recognised when pre-digital criminal forms such as obscenity or fraud are satisfied, but the production and distribution of synthetic content itself is unregulated.

[47] Regulation (EU) 2024/1689, art. 52.
[48] SANJAY TANEJA ET AL., *DEEPFAKE TECHNOLOGY DILEMMAS: MASTERING MANAGERIAL NAVIGATION* 87 (Apple Academic Press 2025).
[49] *Deepfake democracy: Behind the AI trickery shaping India's 2024 elections* (Al Jazeera, 20 February 2024).

These instances show that while traditional offences are prosecuted, the creation of synthetic identities remains untouched regardless of the harm they cause. The easy access to the tools that create such harm makes it even worse.

3.2 The Legal Anonymization

The risk is further enhanced because these offenses are legally anonymized. There is:

i. No legal definition of synthetic media or AI impersonation under Indian law.

ii. No watermarking requirement for AI-generated content to differentiate it from original media.

iii. No offense created for deepfake or voice clone generation or distribution unless it leads to a standalone punishable act (e.g., fraud, defamation).

iv. No AI-specific framework for handling evidence to decide admissibility or contest authenticity in court.

While India's current laws can deal with the effects of deepfake or voice clone abuse for instance, fraud (Section 318(4) of BNS, 2023[50]), defamation (Section 356 BNS, 2023[51]), or obscene electronic content (Section 67[52] of the IT Act) , they fail to criminalize the production, ownership, or sharing of synthetic content per se.

This implies that creating a deepfake or a voice clone, even for nefarious reasons, isn't a criminal offense unless it results in an outcome with legal standing. Voice clone creators employed in scams, or makers of deepfakes of pornographic content, are seldom charged if they aren't directly participating in causing the ultimate harm.[53] This gap in the law encourages criminals and doesn't deter upstream synthetic media creation.

As a result of the emotional, reputational, and national security risks of AI-generated impersonation, there is an immediate need for:

[50] Bharatiya Nyaya Sanhita, 2023, § 318(4), No. 45, Acts of Parliament, 2023 (India).
[51] Bharatiya Nyaya Sanhita, 2023, § 356, No. 45, Acts of Parliament, 2023 (India).
[52] Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).
[53] Hurley, *supra* note 41.

i. A well-defined term of synthetic content, particularly deepfakes and voice clones.

ii. Distinct criminalisation of production and dissemination of said content, regardless of ensuing harm.

iii. Obligatory watermarking or disclosure obligations for AI-produced media.

iv. An independent takedown process and evidence standard for courts, electoral authorities, and law enforcement.

v. Legal enforcement of AI-generated identity abuse as a digital impersonation or forgery.

Briefly, India needs to enact proactive legislation criminalising the employment of AI for fraud, rather than its effects. A proactive stance in regulation is desirable; it is necessary to protect digital integrity in the age of AI.[54]

3.3 Judicial Recognition

The Delhi High Court, in the case of ***Chaitanya Rohilla v. Union of India***[55], went as far as to recognize the legal void within which AI-generated synthetic content such as deepfakes operate. Addressing manipulated audio-visual content and its potential for abuse, the court called for an immediate robust regulatory framework to counter such harms.[56] The verdict specifically cited the "technologically seamless yet legally invisible nature" of deepfakes, emphasizing that current IT law such as Section 67 of the IT Act are reactive and inadequate.[57] The court also raised the prospects of abusing synthetic impersonation in elections, pornography, and blackmail, tracing the international trends of deepfake-based crimes. While admitting the acknowledgment, the court regretted the lack of explicit statutory instruments in India to actively criminalize or regulate such synthetic content.This judicial remark brings decisive heft to the contention that Indian law still has not developed to the extent needed to address the advanced challenges presented by deepfake technologies.

India's constitutional jurisprudence provides strong tools to evaluate the lawfulness of state

[54] Himendra Balalle & Sachini Pannilage, Reassessing Academic Integrity in the Age of AI, 11 SOC. SCI. & HUMAN. OPEN 101299 (2025).
[55] Chaitanya Rohilla v Union of India 2024 DHC (LNINDORD 2024 DEL 1213)
[56] Id.
[57] Id.

(in)action, notably through the prism of the proportionality test fashioned ***in Justice K.S. Puttaswamy v. Union of India (2017)[58].*** The test asks for any limitation on fundamental rights to be legitimated by law, be in pursuit of a legitimate state purpose, and be both essential and proportionate. However, the lack of any legal instrument to control or limit the production and sharing of deepfakes or voice clones leads to a vacuum in which privacy, according to Article 21[59], is systematically eroded without oversight. In ***Navtej Singh Johar v. Union of India (2018)[60],*** individual dignity as a core value was stressed by the Supreme Court in preserving constitutional morality. Now, AI-powered impersonations usually target women and minorities, attacking their very dignity in online forums. The unregulated dissemination of synthetic media infringes not just informational privacy but also the right to a dignified online persona, a natural extension of Puttaswamy and Navtej. Additionally, to the extent that the argument is extended to access to genuine information, ***Anuradha Bhasin v. Union of India (2020)[61]*** enhances that excessive restrictions, or governmental inaction in the midst of technological disinformation, undermine democratic accountability. All these cases put together call for a more constitutionally coherent regulatory approach to AI harms.

3.4 Government's response to this new threat

The government has made step-by-step regulatory moves under the Information Technology Act, 2000, and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, to handle the threats and harm caused by AI, but still, it is not sufficient. The provisions bind intermediaries, particularly social media websites, from hosting, transmitting, or storing illegal content, now expressly including misinformation, impersonation, and material that deceives or misleads.[62] The Ministry of Electronics and Information Technology (MeitY) has also released several advisories instructing platforms to detect and delete synthetic media, such as deepfakes, within 36 hours from the point of reporting. Non-compliance could lead to the loss of safe harbour under Section 79 of the IT Act, invoking Rule 7, by which affected parties can approach the law through the BNS.[63]

Concurrently, CERT-In has issued advisories (May 2023 and Nov 2024) on threats related to

[58] Puttaswamy, (2017) 10 SCC at 497.
[59] Constitution of India 1950, art 21
[60] Navtej Singh Johar v Union of India (2018) 10 SCC 1.
[61] Anuradha Bhasin v Union of India (2020) 3 SCC 637.
[62] *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021*, Ministry of Electronics and Information Technology, Notified via GSR 139(E), 25 February 2021.
[63] Government of India, Government Takes Measures to Tackle Deepfakes (Apr. 4, 2025).

AI, such as deepfakes, providing technical countermeasures and awareness strategies.[64] Additionally, open-namespace initiatives such as the Cyber Swachhta Kendra, Cyber Crime Reporting Portal, and campaigns such as Cyber Jagrookta Diwas are instances of non-legislative activities against the social impact of synthetic content.[65] Yet, these are still reactive and patchy, depending on current cybercrime definitions instead of a specific provision for deepfakes as a new offence.[66] The response of the Government, while changing, is mostly advisory in character, without a strong statutory model that defines and criminalises AI-forged impersonation outright

3.5 Ministerial Words

While India is lagging in legislating deepfake-specific laws, a few ministers have tried to highlight the problem. For example, Minister of State for Electronics & Information Technology, Shri Rajeev Chandrasekhar, has flagged the importance and urgency of action. During Digital India dialogue in November 2023, with platform intermediaries, he stated that "Platforms… will ensure that ... all contracts with users expressly forbid the 11 types of content in the IT Rules,"[67] and that a Rule 7 compliance officer would soon be appointed to support users in reporting violations" he also emphasized that "Deepfakes are a major violation and harm women in particular… It is a legal obligation for platforms to remove such content within 36 hours… failure will attract Rule 7 consequences."[68] Even the Prime Minister acknowledged the growing threat of deep fakes and voice clones and urged that the media and government should take steps to make citizens aware of the risks of synthetic media. Following this, the IT minister Ashwini Vaishnaw regarded deepfakes as a **direct threat to democracy**, pledging platform accountability and potential penalties for noncompliance.[69]

Even with increasing ministerial recognition and action based on advisories, India's present regulatory framework remains predominantly non-binding, disconnected, and responsive. The advisories under the IT Rules, 2021 are founded substantially on self-regulation by intermediaries and lack legislative force, thus leading to uneven enforcement and weak deterrence.[70] There remains no specialized legislation that makes it criminal to produce or spread

[64] Id.
[65] Ministry of Electronics and Information Technology, *Cyber Swachhta Kendra* (Government of India) https://www.meity.gov.in/content/cyber-swachhta-kendra.
[66] Id.
[67] Rajeev Chandrasekhar, Ministry Issues Second Advisory to Online Platforms to Remove Deepfake Content (Nov. 7, 2023).
[68] Id.
[69] Ashwini Vaishnaw, Deepfakes Are a Direct Threat to Democracy (Nov. 3, 2023).
[70] Ministry of Electronics and Information Technology, *Advisory to Intermediaries for Tackling Deepfakes and*

deepfakes or synthetic content in and of themselves, nor are there binding limits on the application of AI to impersonation, biometric cloning, or disinformation campaigns. In contrast to places like Japan or the EU, which make mandatory watermarking, norms of disclosure, and penalties for non-compliance, among their obligations, India still views the abuse of AI as incidental to existing offenses, instead of a specific harm necessitating specific legal protection. In the absence of enforceable provisions, limited usage requirements, and law-defined synthetic media, India's digital policy architecture is lacking in being able to provide substantive protection to victims or hold platforms and developers accountable.[71]

JURISDICTIONAL ANALYSIS: A COMPARATIVE STUDY

As India struggles with the growing incidence of harms brought about by AI, going from money scams with the help of voice clones to reputational injuries through deepfakes, admittedly, the current legal remedies prove to be woefully inadequate. Indian law today offers criminal penalties for the effects of such activity, like fraud under the Indian Penal Code or obscenity under the IT Act, but not the act of creating or disseminating synthetic content per se, especially when consent has not been taken or harm caused. Around the world, however, jurisdictions have moved to criminalize deepfake technology and voice cloning devices and oblige AI developers and platforms to provide transparency, risk mitigation, and responsible usage.[72]

A comparative analysis of AI legislation in different countries in this context provides valuable input for how synthetic media, automatic decision-making, and data manipulation can be more effectively regulated. Regulations in the European Union, the United States (via state initiatives), and China have all enacted legislation to shield data subjects against AI attacks, impose responsibility on developers and deployers, and support trust in digital processes.[73] Their legal approaches, varying from deepfake labelling requirements to biometric data consent structures, can be a necessary point of reference in bolstering India's legal framework against AI-driven threats.

This comparative examination points out how these jurisdictions have sought to fill regulatory

Misinformation (PIB, 7 November 2023) https://pib.gov.in/PressReleasePage.aspx?PRID=1970072.

[71] Id.

[72] Nibedita Basu and Rhishikesh Dave, 'Comparative Analysis of Laws in AI' (2025) 5 *SDGsReview* e05575, 1–23.

[73] Francisca Romana Nanik Alfiani and Faisal Santiago, 'A Comparative Analysis of Artificial Intelligence Regulatory Law in Asia, Europe, and America' (2024) 204 *SHS Web of Conferences* 07006 accessed 18 July 2025

loopholes around AI abuse, deepfakes, and data protection, as well as lessons relevant to India's legislative agenda.

4.1 European Union And India

The European Union has become a world leader in regulating artificial intelligence, data protection, and synthetic material such as deepfakes and voice clones ahead of time. It provides two frameworks, the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (2024), which is designed for a harmonious legal environment for ensuring that AI technologies do not affect the fundamental rights, especially in situations involving manipulation, impersonation, and unauthorized use of data.[74]

Though GDPR and India's DPDP Act, 2023 regulate personal data and lay down regulations for the digital protection of personal data, the ability of both acts to respond to AI threats is different. ***The GDPR provides a definition of personal data under Article 4(1)[75] explicitly, which includes any information relating to an identifiable individual, which extends to voice recordings, facial images, and biometric identifiers.*** Article 9[76] of the GDPR specifies biometric data as sensitive, which requires explicit consent for even lawful use. This assurance and regulation gives individuals a legal foundation to challenge the unauthorised use of their likeness or voice in AI-generated content such as deepfakes or voice clones.

By comparison, the DPDP Act makes no distinction between types of personal data. It does not mention biometric data, facial scans, or voice prints as needing special protection. Section 6(2)(a)[77] allows for processing publicly accessible personal data without consent, which opens a loophole in the sense that voice samples or images uploaded to social media might be legally scraped and utilized for AI training or impersonation, without the knowledge or remedy of the data principal.[78] Therefore, although GDPR's purview does indirectly provide for regulation of synthetic identity abuse, the DPDP Act does nothing on this score unless the same amounts to another penal offence like fraud or obscenity.

[74] Giovanni Sartor and Francesca Lagioia, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence* (EPRS | European Parliamentary Research Service, June 2020) PE 641.530 accessed 18 July 2025
[75] Regulation (EU) 2016/679, art. 7.
[76] Regulation (EU) 2016/679, art. 9.
[77] Digital Personal Data Protection Act, 2023, § 6(2)(a), No. 22, Acts of Parliament, 2023 (India).
[78] Chitranshi S, 'The Deepfake Conundrum: Can the Digital Personal Data Protection Act, 2023 Deal with Misuse of Generative AI?' (2023) *Indian Journal of Law and Technology* accessed 12 July 2025

Though the GDPR and India's DPDP Act, 2023, seek to establish data protection rights, each of these pieces of legislation is confronted by the same technical challenge when applied to AI systems, namely the withdrawal of consent and data erasure. Once voice samples or facial photos are employed to train AI models, such information is integrated into the model's architecture, usually as abstract neural network weights. This renders deletion or retrieval technically impossible.[79] Article 17[80] of the GDPR provides the right to erasure to individuals. ***Though it cannot assuredly delete from AI models in every instance, it obligates data controllers to make "reasonable steps" towards restricting further damage.*** In addition, GDPR's privacy by design, data minimisation, and data protection impact assessments provide an organised framework to minimise the likelihood of unauthorised use before an incident can occur.[81]

The EU Artificial Intelligence Act (2024) specifically targets the risks posed by deepfakes and voice clones.[82] It puts AI systems into four categories: unacceptable, high-risk, limited, and low-risk. Unacceptable AI systems, such as social scoring, real-time biometric monitoring, or subliminal influence, are strictly forbidden. ***Deepfakes are "limited risk,"[83] and Article 52[84] the Act requires that all content created or manipulated by AI (including deepfakes, synthetic videos, or voice simulation) be labeled clearly.*** Not doing so will incur penalties of up to €35 million or 7% of worldwide turnover, which is among the strongest regimes in the world.[85]

Conversely, India's DPDP Act lacks a labelling provision for deepfakes, a definition of synthetic content, redress for persons harmed by impersonation or doctored media, structured risk classification, or pre-market approval for AI systems.[86] India should adopt recommendations from the EU model by incorporating compulsory watermarking, transparency obligations on generative AI, and pre-emptive DPIA protocols.[87]

[79] Laith Alzubaidi et al., Review of Deep Learning: Concepts, CNN Architectures, Challenges, Applications, Future Directions, 8 J. BIG DATA 53 (2021).
[80] Regulation (EU) 2016/679, art. 17.
[81] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Version 2.0 (20 October 2020) accessed 15July2025
[82] Artificial Intelligence Act, art. 52.
[83] Id.
[84] Id.
[85] Artificial Intelligence Act, art. 52.
[86] Swanand Bhale, *Deepfake Laws in India: The Need for Legal Regulation in the AI Era* (SSRN, 1 February 2025) accessed 12July2025
[87] Felipe Romero Moreno, Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights, 58 COMPUT. L. & SEC. REV. 106162 (2025).

The EU's dual regulatory approach, GDPR for personal data and the AI Act for algorithmic responsibility, forms a benchmark for regulating the risks of synthetic content. Its focus on prevention, labelling, and proportionality forms a blueprint that India might while making its own regulation for AI-facilitated impersonation and deception.

4.2 United States And India

The United States does not have a federal AI law but has significant state-level legislation for deepfakes, voice cloning, and synthetic fraud. This legislation, alongside ongoing Federal Trade Commission (FTC) and executive measures by the White House, helps to fill the gap in the evolving regulatory framework.[88]

1. **CALIFORNIA**: This legal distinction is significant. California treats certain types of deepfake generation as inherently wrongful, recognising that AI impersonation can violate privacy, autonomy, and electoral integrity. Indian law, by comparison, remains reactive, responding only when deepfake content causes an identifiable legal injury. Without recognising synthetic identity manipulation as a legal harm, India's current data protection and cybercrime framework leaves critical AI-related abuses unregulated and victims without recourse unless other specific offences can be invoked.[89]

By comparison, India's law does not autonomously criminalise producing or distributing deepfakes, pornographic, political, or otherwise. Neither the IT Act, 2000, nor the Digital Personal Data Protection Act, 2023, contains any definition or provision outlawing the creation of AI-generated synthetic content. If a deepfake is obscene, it could be penalized under Section 67 of the IT Act, and if it is cheating or defamation, such consequences can be charged under the BNS, 2023. However, no law considers simply pretending to be a person through AI illegal, even though the deception or intrusion is manipulative. The Indian strategy thus continues to be consequence-oriented, targeting only the consequence of using a deepfake, not the use of creating synthetic material in the first place.[90]

This is a legal distinction that matters. California addresses some forms of deepfake creation as wrongful by nature, acknowledging AI impersonation can itself cause harm to privacy,

[88] Staff (Office of Technology and Division of Advertising Practices), "AI and the Risk of Consumer Harm" (Federal Trade Commission, 3 January 2025) accessed 14 July 2025
[89] California Assembly Bill 2655 (Defending Democracy from Deepfake Deception Act of 2024) (Cal 2024)
[90] Romero Moreno, *supra* note 82.

autonomy, and election integrity. Indian law, contrastingly, is reactive, acting only if deepfake content results in a discernible legal harm. By failing to recognize synthetic identity manipulation as a legal harm per se, India's existing data protection and cybercrime structure leaves pivotal AI-associated abuses unregulated and victims with no remedy unless other particular offences may be called upon.[91]

2. **ILLINIOS:** Illinois' Biometric Information Privacy Act of 2008[92] (BIPA), also known as BIPA, does not once use the words "deepfake" or "voice cloning". However, it remains one of the most potent and appropriate legislative weapons for combating AI-created synthetic impersonation. BIPA explicitly regulates the collection, storage, and use of biometric identifiers, defining them in Section 10[93] to include facial scans, voiceprints, retina scans, and hand geometry, the same building blocks commonly used to train AI systems that create deepfakes and cloned voices. While BIPA does not legally forbid the creation of deepfakes in and of themselves, it sets onerous requirements for any organization looking to obtain biometric data, including required informed written consent under Section 15(b)[94] and (c)[95], notice of purpose and storage duration, and compliance with data protection. This law has been effectively used in high-profile cases against AI and synthetic media, including Clearview AI for scraping billions of face photos from social media sites without users' permission to develop facial recognition software and TikTok for harvesting face geometry through filters and algorithms.[96] Although these instances did not concern deepfakes per se, the training materials adopted by such AI systems considerably overlap with the information BIPA aims to safeguard. Essentially, BIPA provides indirect but enforceable regulation of deepfake technology by closely regulating the legal utilization of biometric data at source.[97]

India's DPDP Act, 2023, provides no nuanced or sensitive handling of biometric data. The Act does not separately define biometric identifiers or categorize them as "sensitive personal data." Furthermore, Section 6(2)(a) allows for processing publicly available personal data without consent, arguably covering voice clips and facial photos posted online. This provides a

[91] Rachit Tiwari, 'Legal Recognition of Deepfake Offences in India: A Regulatory Gap in the AI Age' (2024) 8(2) *National Law Review* 112
[92] Biometric Information Privacy Act, 740 Ill Comp Stat 14 (2008)
[93] Biometric Information Privacy Act, 740 Ill Comp Stat 14/10 (2008)
[94] Biometric Information Privacy Act, 740 Ill Comp Stat 14/15(b) (2008)
[95] Biometric Information Privacy Act, 740 Ill Comp Stat 14/15(c) (2008)
[96] Bianca Bhatti, 'Clearview AI to Pay $20 Million in BIPA Settlement for Facial Recognition Scraping' (Reuters, 11 March 2024) accessed 22July 2025
[97] Biometric Information Privacy Act, 740 Ill Comp Stat 14 (2008)

regulatory gap whereby biometric data of Indian users, social media available to all publicly posted, may be legally scraped and employed for training deepfake and voice cloning models without legal prohibition or consent requirement. In comparison with BIPA, the DPDP Act does not have a private right of action or statutory damages, with individuals having no effective recourse if their biometric identity is used to enable synthetic impersonation.

Illinois has proven that, though it does not explicitly regulate deepfakes, its biometric privacy framework has proven instrumental in preventing raw data from being misused, and its success in enforcement offers a model for India to emulate if it intends to build a truly protective digital ecosystem.

3. **NEW YORK:** New York is one of the first US jurisdictions to directly recognize and regulate AI-created impersonation and deepfakes, particularly in terms of sexual exploitation and posthumous image rights. The state added to its Civil Rights Law[98] in 2020 to criminalize the production, distribution, and publication of sexually explicit deepfake images without the consent of the person depicted, under Section 50-f.[99] The statute also extends to digitally manipulated photos, videos, or sound made through artificial intelligence. New York further enacted post-mortem publicity rights under Sections 50[100] and 51[101], which place the deceased's estates in control of their digital image for 40 years following death. This aims explicitly at synthetic imitations of celebrities, performers, or individuals in commercial, entertainment, or advertising purposes, thus acknowledging AI-based reanimation as a legally sensitive activity.[102]

In addition to criminalisation, New York's law also serves as a privacy-protective model for all those using and entering the dangers of deep learning, facial synthesis, and voice cloning technologies. In acknowledging a right to be in control of one's image, voice, and likeness, even posthumously, the legislation extends the classical boundaries of informational privacy into the field of digital identity.[103] The incorporation of civil remedies and injunctive relief, even in the absence of financial damage, gives victims of abuse of synthetic media the power to promptly seek redress from the law. This legal framework recognizes that synthetic impersonation through deepfake pornography, AI-created political speeches, or false endorsements not only creates

[98] Civil Rights Act of 1964, 42 USC § 2000a et seq
[99] Civil Rights Act of 1964, 42 USC § 2000e–5
[100] NY Civil Rights Law §§ 50 (McKinney 2021)
[101] Id.
[102] RAISE Act (S 6953B/A 6453B) (NY State Senate and Assembly, passed Senate 12 June 2025)
[103] Sentinella and Zweifel-Keegan, *US State AI Governance Legislation Tracker* (IAPP, last updated 1 July 2025) accessed 22 July 2025.

reputational but also emotional and psychological damage. New York's system thus integrates both privacy enforcement and dignity protection, balancing the legal system with the emerging dangers of generative AI.[104]

On the other hand, India's existing legal system has no specific protection for deepfakes or AI-assisted impersonation. The DPDP Act, 2023, does not define or govern synthetic content, deepfakes, or biometric impersonation, nor does it offer any protection against using AI in replicating or altering an individual's identity.[105] While crimes such as defamation, fraud, and obscenity can be prosecuted under the BNS, 2023, or the Information Technology Act, they deal with only the results of AI misuse, not the process of synthetic creation itself. There is no posthumous protection of digital identity, no content labelling or AI-disclosure requirement, and no explicit victim protections for voice cloning or deepfake images. This void denies Indian citizens, and especially women, public figures, and vulnerable persons, adequate measures to prevent or counter AI-engineered impersonation, rendering the legal framework reactive instead of preventive in the age of fast-developing technological threats.[106]

Due to these lacunae, India must go beyond reactive legislation and implement proactive laws dealing with AI-facilitated impersonation and synthetic media harms. Taking reference from New York, India needs to prioritize bringing legislation for deepfakes, voice, and other AI-related identity theft activities.

3.3 China and India

China is now one of the few significant jurisdictions globally to possess pervasive and enforceable laws targeting specifically deepfakes, voice cloning, and generative AI.[107] The "Provisions on the Administration of Deep Synthesis Internet Information Services"[108], which entered into effect on 10 January 2023, were published by the Cyberspace Administration of China[109] (CAC) and are the first of their kind worldwide. These measures establish "deep synthesis" to encompass AI technology that synthesizes or manipulates voice, video, or image

[104] Id.
[105] MITTAL, *supra* note 20, at 212.
[106] Amlan Mohanty and Shatakratu Sahu, *India's Advance on AI Regulation* (Carnegie India, 21 November 2024) accessed 19July2025
[107] Mimi Zou and Lu Zhang, 'Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models' (2025) 1 *Cambridge Forum on AI: Law and Governance* e8 accessed 22July 2025
[108] *Provisions on the Administration of Deep Synthesis Internet Information Services* (Cyberspace Administration of China, 10 January 2023)
[109] Id.

content to impersonate actual individuals. Independently, the "Interim Measures for the Management of Generative Artificial Intelligence Services"[110], effective 15 August 2023, regulate AI programs such as chatbots, synthetic audio and video platforms, and facial recognition systems. All these frameworks combine to build a strong regulatory system for managing, monitoring, and curbing the abuse of AI for generating online content.[111]

These Chinese laws are not just declaratory; they have precise, enforceable protections that lower the risks of AI-facilitated harms. Sites providing deep synthesis services must apply mandatory 7278abelling or watermarking of all AI-produced content to notify audiences when they view synthetic content.[112] When an individual's personality, voice, or identity is applied in AI-produced content, sites need to get advanced permission from that individual. Also, platforms should be required to establish users' identities, maintain usage logs, perform content moderation, and provide transparency in complaint and takedown procedures to forestall abuse. The legislation effectively places responsibility on both developers and service providers, precluding crimes like deepfake pornography, voice phishing fraud, impersonation, and AI-generated disinformation. These laws also ban AI-created content that endangers national security, public order, or human dignity and compel generative AI systems to employ legally acquired training data, further shutting loopholes in other jurisdictions that are commonly abused.[113]

Though China's Provisions for Deep Synthesis Internet Information Service Management[114](2023) operate as rules, these are underpinned by stern enforcement powers that rise to criminal prosecution when required. The Provisions empower administrative action such as warning, content removal, suspension of business, blocklisting of service providers, and penalties for firms or individuals who do not comply with content labelling, consent, and safety requirements. Yet, the case is forwarded to public security organs according to China's Criminal Law, where offenses are discovered to be criminal offenses, like impersonation, spreading false

[110] *Interim Measures for the Management of Generative Artificial Intelligence Services* (Cyberspace Administration of China and others, 15 August 2023) arts 1–23

[111] Sara Migliorini, 'China's Measures on Generative AI: Origin, Context and Significance' (2024) *Computer Law & Security Review* accessed 21 July 2025

[112] *Regulations on the Administration of Deep Synthesis of Internet Information Services* (Cyberspace Administration of China, Ministry of Industry and Information Technology and Ministry of Public Security, adopted 25 November 2022, effective 10 January 2023)

[113] Covington & Burling LLP, 'Labeling of AI Generated Content: New Guidelines Released in China' (Inside Global Tech, 30 August 2023)

[114] Nat'l Info. Sec. Standardization Tech. Comm. (TC260), *Standard Practice Guide: Coding Rule for Service Providers of Network Security Artificial Intelligence Generated Synthetic Content Label (Draft for Comment)* (Jan. 22, 2025).

information, or illegally handling personal information.[115] For instance, Article 253[116] criminalizes the illegal obtaining, sale, or supply of personal information with a seven-year jail term as the punishment. Article 291A[117] criminalises the creation or dissemination of false information, the central issue with deepfakes aimed at causing unrest or influencing public opinion. Secondly, if synthetic content is employed in defamation (Article 246[118]) or pornographic dissemination, additional criminal liabilities exist. China's enforcement authorities have taken action against several platforms carrying or not policing AI-generated content, and taken legal action in the deepfake impersonation of government officials.[119] The various levels of the enforcement system, ranging from administrative deterrence to criminal punishment, demarcate China's robust legal commitment to inhibiting and punishing AI-facilitated content manipulation.

Conversely, India does not have a specific and enforceable legal regime for dealing with the production, dissemination, and manipulation of AI-created synthetic content.[120] Whereas China's deep synthesis rules specify labelling, prior approval, developer responsibility, and penal liability, Indian law is scattered. The DPDP Act, 2023, does not cover synthetic content, deepfakes, or impersonation using AI.[121] Current legislations such as the IT Act, 2000, and BNS, 2023, touch upon only the downstream harms, defamation, fraud, and obscenity, without regulating the technology process or platforms facilitating them. India doesn't mandate watermarking AI content, place proactive obligations on platforms, or criminalize AI-based non-consensual use of identity.[122] Additionally, post-mortem digital rights, standards of consent, and developer responsibilities are untouched, providing few options for victims of deepfakes and voice clones. India's legal reaction is still predominantly reactive, relative to China's multi-level enforcement system, with no administration or criminal framework specific to AI-facilitated manipulation.[123]

India must embrace an integrated legal regime in the mould of China's forward-looking model to meet the growing abuse of generative AI. This entails obligatory content tagging, consent,

[115] *Criminal Law of the People's Republic of China* (adopted 1 July 1979, revised most recently 2020)
[116] *Criminal Law of the People's Republic of China* (adopted 1 July 1979, revised 2020), art 253
[117] *Criminal Law of the People's Republic of China* (adopted 1 July 1979, revised 2020), art 291A
[118] *Criminal Law of the People's Republic of China* (adopted 1 July 1979, revised 2020), art 246
[119] Sara Migliorini, 'China's Measures on Generative AI: Origin, Context and Significance' (2024) *Computer Law & Security Review* accessed 22July2025
[120] Id.
[121] Id.
[122] Romero Moreno, *supra* note 82.
[123] Id.

developer responsibility, and criminal sanctions for synthetic abuse. Failing timely reform, India stands to fall behind in safeguarding its citizens' digital identity, dignity, and democratic integrity.

5. KEY CASES DEFINING THE NEED FOR AI LEGISLATION

5.1 Voice Cloning Scams

In late 2023, cases of a stunning surge in UPI-based financial frauds carried out employing voice clones generated with the help of AI came to light in Noida and Hyderabad.[124] Cyber fraudsters obtained short audio recordings of victims' kin through social media videos or WhatsApp voice messages and then employed voice-cloning technology to mimic distress calls. In one instance, a woman sent ₹48,000 after being threatened by a call from a person who was impersonating her son's voice, alleging that he was involved in an accident. When the fraud was detected, the money had already been diverted into several untraceable wallets.[125]

Despite the evident impersonation, no law outright criminalized voice cloning as an act. Additionally, since voice samples were scraped from public content, the DPDP Act, 2023, is not applicable under Section 6 exceptions, which leave out public data.

This key policy lacuna ensures that synthetic impersonation is not criminalized in India. There is no requirement for AI businesses to avoid misuse or watermark content they produce. Nor are entities like ElevenLabs, which sell voice cloning software worldwide, subject to any direct regulation under Indian law. Consequently, users have no straightforward avenue for redress against harms occasioned by "lawful-looking" synthetic misuse.

5.2 Deepfake Pornography

In March 2024, an Indian university student found that her Instagram photos were used without permission to generate deepfake pornographic images that circulated in Reddit and Telegram communities. Even though she registered a police complaint, the action was only to register one under Section 67 of the IT Act (obscenity) and Sections 74[126] and 77[127] of the BNS,

[124] *Family Member in Distress or an AI Voice Clone?, SCROLL.IN (Dec. 18, 2023).*
[125] *Woman Gets SOS from 'Nephew' in Canada, Loses Rs 1.4 Lakh to AI Voice Fraud, TIMES OF INDIA (Nov. 16, 2023).*
[126] Bharatiya Nyaya Sanhita, 2023, § 74, No. 45, Acts of Parliament, 2023 (India).
[127] Bharatiya Nyaya Sanhita, 2023, § 77, No. 45, Acts of Parliament, 2023 (India).

2023(voyeurism and insult to modesty). The case pointed out two significant loopholes:

- To begin with, Indian law does not criminalize the act of producing deepfakes unless they are obscene or defamatory. Even when AI tools use explicit deepfakes, the act is not punishable unless the user shares them with others. This extends legal immunity to creators of private deepfakes, a fast-growing concern everywhere.[128]

- Second, the sites that host such content, most of which are offshore-hosted, are shielded under Section 79 of the IT Act, which provides intermediary liability immunity unless the site "knowingly" hosts unlawful content. Without watermarking or identification requirements for AI-generated content, sites can plead ignorance and pass the burden to the victim to establish malice or intent.[129]

This loophole provides no viable solution to most victims. Even though the DPDP Act permits complaints against data fiduciaries, it provides no recourse for synthetic outputs generated using publicly scraped data, making it useless in those instances.

6. DIGITAL GOVERNANCE AND CONSTITUTIONAL MORALITY

6.1 The Right to Privacy in the Digital Age

Another serious constitutional issue is the extensive application of deepfakes to produce non-consensual pornographic content, especially against women and children. Deepfake pornography not only infringes privacy but also the right to dignity under Article 21. The courts have always insisted that dignity is not merely refraining from physical harm but protection from mental trauma, humiliation, and reputational assault.[130]

In reality, though, victims of deepfake pornography do not get much respite. Recent Indian cases demonstrate that FIRs are usually lodged under Section 67 of the IT Act or Sections 354A, 354C, and 509 IPC, but these sections do not apply if the action does not involve actual nudity, even though the psychological, social, and emotional damage is equally serious. The lack of criminalising the creation of synthetic media leaves the creator relatively free from sanction,

[128] Kshitija Kashik, *Navigating the Future: India's Strategic Approach to Artificial Intelligence Regulations* (Research Paper, National Centre for Good Governance 2025).
[129] Id.
[130] INDIA CONST. art. 21.

except where the content is shared or goes viral.[131]

This is in direct contrast to the UK and Australia, which are updating their sexual offences legislation to encompass synthetic pornography irrespective of whether real pictures were involved.

6.2 Dignity and bodily integrity in the AI era

The K.S. Puttaswamy v. Union of India[132] (2017) highlighted the right to privacy as a constitutional right under Article 21[133]. The Court said that privacy includes the right to shape one's identity, personal information, bodily integrity, and informational autonomy. Yet, deepfakes and voice clones destroy this right on all fronts. Current AI can replicate a human's face, voice, body language, and words, often from publicly available data, but not necessarily consented to being used in this manner.

For example, if one AI system copies a person's voice from a public video and then uses it in a scam call, the laws in India currently (e.g., Section 66D of the IT Act or Section 420 of the IPC) can penalize the result (cheating), but not the process of virtually impersonating someone without his consent. This creates a legal gap in today's legislation in which people have no redress for the very act of digital cloning, apart from its blatant disregard for their identity, autonomy, and dignity.[134]

This conflicts with the EU Charter of Fundamental Rights and the GDPR, which both maintain an individual's right of objection to processing, profiling, and automated decisions. Indian law does not have a similar framework. The Digital Personal Data Protection Act, 2023, though dealing with consent, does not deal with synthetic content or place obligations on platforms or developers enabling impersonation.

7. URGENT NEED FOR AI LEGISLATION

In light of these multidimensional constitutional harms, India needs to proceed with

[131] UNIVERSAL'S CONCISE COMMENTARY ON INFORMATION TECHNOLOGY 145 (1st ed., Universal Law Publishing Co. Pvt. Ltd. 2016).
[132] Puttaswamy, (2017) 10 SCC at 497.
[133] INDIA CONST. art. 21.
[134] Swanand Bhale, *Deepfake Laws in India: The Need for Legal Regulation in the AI Era* (SSRN, 25 April 2025)

criminalizing:

- The unauthorized creation or possession of deepfakes or synthetic voice duplicates,
- The use of synthetic content with the purpose of deceiving, manipulating, or defaming,
- The designing and marketing of AI solutions that enable impersonation in the absence of security measures.

This does not equate to suppressing innovation; instead, it enforces ethical innovation. The laws need to be drawn up to keep malicious abuse separate from creative or satirical content by concentrating on intent, consent, and harm potential.[135] This can be done by:

- Revising the Information Technology Act, 2000 to clearly define "synthetic content" and punish misuse thereof,
- Enacting a new chapter of the IPC or a separate AI Harms Act addressing specifically AI-based fraud.
- Implementing strict liability on synthetic media tool developers where damage is caused by a lack of adequate safeguards.

India also has to look toward invoking Article 38[136] of the Constitution (DPSP), which requires the State to reduce inequalities and render justice, to support active digital protections. Incorporating constitutional morality into AI governance will see India uphold its digital future not just as innovative but also fair and human.[137]

REPORTS AND SURVEYS

Reports by the Data Security Council of India (DSCI) and advisories issued by CERT-In reveal a growing consensus among stakeholders about the risks associated with deepfake and AI-generated content.[138] According to the DSCI's exploratory note, concerns include increasing

[135] Centre for International Governance Innovation, *Governing Cyberspace during a Crisis in Trust: An Essay Series on the Economic Potential- and Vulnerability- of Transformative Technologies and Cyber Security* (CIGI 2021) https://www.cigionline.org/multimedia/governing-cyberspace-during-crisis-trust/.
[136] INDIA CONST. art. 38.
[137] Id.
[138] Data Security Council of India, *Exploratory Note on Deepfakes: Redefining Reality and the Risks to Safety, Trust, and Accountability* (2024); Indian Computer Emergency Response Team (CERT-In), *Advisory on*

incidents of synthetic impersonation, misuse of biometric data, and the emotional manipulation of users through hyper-realistic audio-visual fakes.[139] Industry meetings organized by MeitY also echo the same concern, platforms indicate increasing difficulty in detecting and removing deepfakes prior to them turning viral. Beyond this, there is also scarce technical capability to track the source of such content, leading to irrevocable reputational and financial loss. All these observations add weight to the imperative of statutory change and anticipatory detection measures even in the lack of direct empirical surveys.[140] Public debate also directed attention to the inefficacy of existing redressal systems, particularly when identity, trust, and consent are breached through AI-facilitated deception.

During 2023 and 2024, MeitY released several advisories to social media intermediaries asking them to remove deepfakes within 36 hours of being notified.[141] These advisories are not legally binding but mere administrative notices based on current IT Rules. The CERT-In advisory (November 2024) emphasized technical guidelines like watermarking, AI-content flagging, and user awareness campaigns but conceded that enforcement is still patchy across platforms. Stakeholders, industry experts and digital rights organizations, have long advocated for the establishment of a single regulatory agency to regulate AI-generated content, issue orders for take-down, and provide relief to victims.[142] Yet there is no single, enforceable mechanism in place. These results indicate a broad awareness of the issue but few coordinated legal tools for its management. The lack of determinate liability regimes and enforceable norms puts the victim at risk, particularly in the context of rapid-moving, faceless AI attacks.

8. WAY FORWARD

The increasing embedment of artificial intelligence in mundane digital life has remapped not only the horizon of innovation possibilities but also the range of harms that people can experience without regulatory protection. In India, although the passing of the Digital Personal Data Protection Act, 2023 was a forward-looking step towards recognizing data rights in the digital era, it is vastly wanting in keeping pace with the peculiar threats that are AI-driven and

Deepfake Threats and Safety Measures (November 2024) https://www.cert-in.org.in/ accessed 5 August 2025.
[139] Id.
[140] Id.
[141] Ministry of Electronics and Information Technology (MeitY), *Union Government Issues Advisory to Social Media Intermediaries to Identify Misinformation and Deepfakes* (PIB Delhi, 7 November 2023) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050.
[142] Id.

include deepfakes, voice cloning, and algorithmic impersonation.[143]

This study showed that India's present legal framework, grounded in the Information Technology Act, 2000, and supplemented by the DPDP Act, is still reactive and disjointed. ***It criminalizes the result of AI abuse (e.g., fraud, defamation, obscenity) but does not criminalize the act of producing or disseminating synthetic content itself.*** This gap deprives victims of a meaningful legal remedy and enables perpetrators to work in legal limbo.[144]

Comparative legal regimes examined, from the European Union's twinned regime (the GDPR and the AI Act) to state legislation in the United States, and pro-active frameworks in China, Singapore, the UK, and Australia, demonstrate a building global consensus: synthetic impersonation must be recognized as a standalone harm, strict requirements must be imposed upon AI developers and platforms, and transparency, traceability, and accountability must be available in AI-generated content.

India can ill afford to lag behind. With its surging digital economy and huge user base, the nation is particularly susceptible to AI-facilitated deception. Without proper legal guidelines and technical protections, voice clones can be employed in financial scams, deepfakes can rig elections, and synthetic pornography can permanently destroy reputations, all with the law watching impotently.[145]

9. KEY RECOMMENDATIONS

1. **Criminalisation of Deepfakes and AI-based Impersonation:** India needs to pass independent legislation on AI harms to squarely criminalise unauthorized synthetic impersonation. This involves the creation, transmission, and storage of content mimicking an individual's likeness, voice, or biometric signature without permission. In ***Chaitanya Rohilla v. Union of India[146] (2024)***, the Delhi High Court recognised the "technologically seamless yet legally invisible" characteristics of deepfakes, which called for immediate legislative intervention. While existing provisions such as Section 67 of the IT Act deal with obscenity, they do not specifically tackle

[143] Aaron A. Funa & Renz Alvin E. Gabay, Policy Guidelines and Recommendations on AI Use in Teaching and Learning, 11 SOC. SCI. & HUMAN. OPEN 101221 (2025).
[144] Recommendation on the Ethics of Artificial Intelligence (UNESCO, adopted 24 November 2021.
[145] Early Ridho Kismawadi, 'The Impact of Deepfakes on Trust and Security in Islamic Banking' in *The Impact of Deepfakes on Trust and Security in Islamic Banking: Emerging Threats and Mitigation Strategies* (IGI Global 2024).
[146] Chaitanya Rohilla v Union of India LNINDORD 2024 DEL 1793

the creation of deepfakes.[147] Moreover, MeitY's advisories to platforms, though forward-thinking, are not backed by enforceable penal provisions, which means criminalisation is imperative to prevent new ways of identity fraud.

2. **Mandatory Watermarking and Disclosure of AI Content:** A legislative mandate must be instituted mandating that all platforms and developers clearly watermark or mark synthetic content visibly. This is borrowed from best practices of Article 52 of the EU AI Act (2024) and China's Deep Synthesis Provisions (2023), both of which provide for transparency in AI-generated content. India's CERT-In advisory (November 2024) alluded to this necessity, but enforceability is still lacking. Incoporating this requirement into law will help both enforcers and users differentiate between real and created content, stemming misinformation and identity falsification.[148]

3. **Strict Platform and Developer Accountability:** Platform operators and AI developers should be strictly liable for damage caused by their tools when they are used for synthetic impersonation or deepfake spreading. The IT Rules, 2021 under Rule 7 already dispense intermediary safe harbour if due diligence obligations are not met.[149] It must be extended to synthetic content proactively as well. Courts such as the Kerala High Court in ***X v. Union of India (2021)***[150] have reaffirmed the role of intermediaries in privacy and dignity cases. By introducing explicit timelines and enforcement penalties for such takedown failure cases with regard to synthetic media, the regulatory system can become preventive as well as responsible.[151]

4. **AI Harms Redressal Cell:** A specialized statutory redressal forum, either within the Data Protection Board or a separate tribunal, should be given the capability to address complaints regarding AI-generated harm.[152] Drawing inspiration from the Grievance Appellate Committees in the IT Rules, 2022, such a forum should be invested with powers to order immediate takedown, provide interim compensation, and conduct expedited hearings. Considering the irreparable reputational harm deepfakes may inflict, redress must be time-bound and

[147] Information Technology Act, § 67.
[148] Indian Computer Emergency Response Team (CERT-In), 'Advisory on Deepfake Threats and Mitigation Measures' (November 2024) https://www.cert-in.org.in/ accessed 5 August 2025.
[149] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 7, G.S.R. 139(E), Gazette of India, Feb. 25, 2021 (India).
[150] X v Union of India (2021) 2 SCC 758
[151] Id.
[152] Ministry of Electronics & IT, *supra* note 141.

technologically facilitated.[153]

5. **Recognition of Synthetic Identity as Personal Data:** The DPDP Act, 2023 must be amended to incorporate digital simulations created synthetically (e.g., deepfakes and AI voice clones) into the definition of personal data when related to an identifiable person. This will allow persons to assert rights to AI-created replicas of their identity. The EU GDPR already guards biometric and inferred data, a robust precedent. Indian constitutional law, particularly Justice ***K.S. Puttaswamy v. Union of India,***[154] has maintained the doctrine of informational autonomy, further lending to such an inclusion.

6. **Directive Principles-Based AI Legislation:** India needs to set its AI regulation in the values of the Constitution, specifically Article 38 (social justice) and Article 51A(h) (scientific temper and humanism).[155] This would uphold ethical usage of AI while fostering innovation responsibly. The NITI Aayog Discussion Paper on AI (2018) also emphasized ethical, inclusive, and rights-based AI development. By basing AI law on constitutional directives, the coming legislation can balance technology and societal welfare meaningfully.[156]

7. **National Awareness and Digital Literacy Campaign:** The government must initiate a focused campaign to inform citizens about AI ills, such as how to recognize, report, and legally counter synthetic content abuse.[157] While CERT-In carries out wide-ranging cyber hygiene campaigns like Cyber Jagrookta Diwas and Swachhta Pakhwada, there is no specific education on AI. Public awareness, in local languages and on multiple platforms, can enable citizens to defend themselves and hold AI creators and platforms accountable.

10. CONCLUSION

Against the backdrop of the monumental potential of AI to empower or hazard, law cannot be an impartial spectator. It has to transform, not just to keep pace with technology but to influence its use appropriately, safeguard basic rights, and ensure the digital dignity of all citizens. India is at a critical crossroads where it either can emerge as a world leader in responsible AI regulation or face a legal crisis that makes its citizens ever more susceptible to hidden algorithmic harms.

[153] Id.
[154] Puttaswamy, (2017) 10 SCC at 598.
[155] INDIA CONST. art. 51A(h).
[156] Ministry of Electronics & IT, *supra* note 88.
[157] Ministry of Electronics & IT, *supra* note 141.

The hour is now, not after the next election has been stolen by a deepfake, not after another family has been cheated by a voice clone, not after reputations have been ruined by fake videos. The law needs to catch up with the machine, and the Constitution needs to catch up with the code.