Page: 583-614 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.286

DEEPFAKES AND GENERATIVE AI IN INDIA: RETHINKING THE LEGAL AND CONSTITUTIONAL FRAMEWORK FOR DIGITAL GOVERNANCE

Omkar Acharya[1] & Shibanee Acharya[2]

I. ABSTRACT

The rapid development of Generative Artificial Intelligence (AI) has transformed digital innovation while raising complex legal and constitutional concerns. Among its most disruptive manifestations is deepfake technology, which enables the creation of realistic synthetic audio, video and images capable of blurring the distinction between fact and fabrication. In India, the misuse of deepfakes has raised serious concerns relating to privacy, misinformation, electoral integrity, cybercrime, defamation, intellectual property, national security and gender-based digital violence. While the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provide partial remedies, they do not fully address the regulatory challenges posed by AI-generated synthetic media. This paper critically examines India's legal framework on deepfakes and Generative AI, particularly in light of fundamental rights under Articles 14, 19 and 21 of the Constitution, and judicial developments concerning privacy, free speech, dignity and digital governance. Using doctrinal and comparative legal research methods, the study also evaluates international approaches, including the European Union AI Act, the Council of Europe Framework Convention on Artificial Intelligence, and selected regulatory measures in the United States and China. It argues for a constitutionally grounded and risk-based AI governance framework that ensures accountability, transparency and protection of individual rights while preserving technological innovation. The paper recommends dedicated AI regulation incorporating algorithmic accountability, mandatory watermarking of AI-generated content, platform liability and institutional oversight mechanisms. The study

[1] LLM, 2nd Semester,Fakir Mohan University, PG Department of Law, Odisha, (India). Email: omacharya@gmail.com
[2] LLM, 2nd Semester,Fakir Mohan University, PG Department of Law, Odisha, (India). Email: shibaneeacharya9798@gmail.com

 (ISSN: 2583-7753)

contributes to digital constitutionalism by proposing legal reforms aligned with Indian constitutional principles and the evolving digital landscape.

II. KEYWORDS

Deepfakes, Generative Artificial Intelligence, Digital Governance, Constitutional Law & Artificial Intelligence Regulation.

III. INTRODUCTION

Artificial Intelligence (AI) has revolutionized the digital landscape with its ability to quickly process and then create highly sophisticated and human-like content. The advent of Generative Artificial Intelligence (Generative AI) has ushered in new technologies capable of generating original text, images, audio recordings, computer code and realistic videos with little or no human input. Generative AI has emerged as a groundbreaking technology with applications in various fields, including education, healthcare, journalism, finance, entertainment, governance, and scientific research, among others, leveraging cutting-edge technologies like Generative Adversarial Networks (GANs), diffusion models, and Large Language Models (LLMs). With its capacity to boost productivity, automate creative tasks, and drive innovation, AI has emerged as one of the most prominent technologies of the 21st century.[3]

As a result of all these unprecedented technological developments, Generative AI has also introduced new and intricate legal, ethical and constitutional issues. Technologies that can develop positive innovations are also able to produce highly realistic synthetic media, which is known as "deepfakes. Deepfakes are intended to be used for digitally altering an audio, image, or video that looks like a real person with the intent of fooling the average viewer. Open-source AI tools and commercial generative platforms have seen a drastic improvement that has significantly reduced the technical hurdles involved in producing deceptive material, thus expanding and deepening the scope of misinformation campaigns, cyber fraud, identity theft, impersonation, financial scams and reputational damage.[4]

[3] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–30 (4th ed. 2021).
[4] Ia n J. Goodfellow et al., Generative Adversarial Nets, in Advances in Neural Information Processing Systems 2672 (2014).

One of the most troubling uses of Generative AI is deepfake technology, which could pose one of the greatest threats to the democratic system and constitutional values. Deepfakes have been used to generate fake videos of politicians, meddle in election campaigning, during communal disputes, to produce intimate images without consent, and to debunk digital evidence. Synthetic media can proliferate quickly across jurisdictions, before verification mechanisms can catch up, due to its viral nature of social media platforms. As a result, the deepfakes have become more than mere examples of digital manipulation; they are now a systemic threat to electoral integrity, national security, public order, judicial administration, and safeguarding fundamental rights.[5]

Currently, India does not have a comprehensive statute that sets out to regulate Artificial Intelligence and synthetic media. In contrast, the law governing such legal rights is scattered across several Acts, such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as well as copyright laws and constitutional principles on privacy and freedom of speech. These laws focus on different facets of cybercrime, obscenity, data protection, and intermediary liability, but they fail to cover the entire range of issues surrounding AI-generated content, algorithmic accountability, transparency requirements, and the duties of AI developers and deployers. This has resulted in very weak, reactive and technologically sub-standard regulatory action.[6]

A. Research Problem

The rapid-growth of Generative AI and deepfake technologies have revealed inadequacies in India's current legal and constitutional framework for digital technologies. Despite the existence of various statutory provisions regulating cyber offences, privacy infringement, intermediary liability and digital communications,

[5] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019).
[6] Information Technology Act, No. 21 of 2000, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).

most of these laws were enacted well before the widespread emergence of advanced AI-generated synthetic media.

As a result, laws on deepfakes are lacking at the moment. Regulatory pressure is mounting due to the vagueness surrounding who is legally responsible for AI-generated content. Current laws offer only limited assistance in assigning liability to various parties, including developers, operators, content creators, deployers, and end-users of AI responsible for harmful synthetic media. Consequentially, Article 19 of the Indian Constitution provides for the freedom of speech and expression as sub-article (1)(a). This right is not absolute. Current laws do not sufficiently protect the constitutional rights to privacy, dignity, and reputation against any non-consensual synthetic media, identity theft and digital impersonation.

Moreover, there is uncertainty about the obligations of intermediaries to detect, identify, remove or stop the spread of content generated by artificial intelligence (AI). The lack of statutory standards on algorithmic transparency, AI auditing, risk assessment, watermarking technologies and disclosure standards has resulted in significant regulatory uncertainty. The problem of deepfake content is aggravated due to jurisdictional issues resulting from the cross-border dissemination of AI-generated content. During elections, these issues may be intensified due to the manipulation of voter perceptions, which may lead to the spread of political disinformation.

The current legal framework of India is fragmented and reactive, which necessitates a holistic framework for AI that encompasses constitutional safeguards, statutory accountability, technological regulation, and international best practices. The present research attempts to critically examine the current Indian laws on deepfakes and generative Artificial Intelligence (AI), look at comparative international regulatory frameworks, and suggest a coherent legal and constitutional framework that can strike a balance between innovative technology on the one hand, and the protection of rights, democratic governance and due digital governance on the other.

B. Research Objectives

The main aim of this study is to analyses the consequent legal and constitutional issues that are being raised in regard to the rising use of Generative Artificial Intelligence (AI) and deepfake technologies in India. The technological evolution of Generative AI

and its increasing ramifications for governance, communication, democratic processes, and digital rights will be traced. The study will further examine the constitutional consequences of AI generated data to guarantee equality, freedom of speech and expression, privacy, dignity, and due process as guaranteed by Articles 14, 19, 21 of the Constitution of India.[7]

The adequacy of the existing laws like the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, intermediary liability, etc. will also be critically analyzed.[8] In addition to this, it analyses judicial responses to privacy, misinformation and digital constitutionalism, besides a comparative study of international regulatory frameworks of AI. The objective of the investigation is to identify regulatory shortcomings relating to accountability, transparency, algorithms, civil and criminal liability, and propose a legal framework for regulation of Generative AI and deepfakes in India that is constitutionally compatible, rights-based and risk-based.[9]

C. Research Questions

The speedy evolution of Generative Artificial Intelligence (GenAI) and deepfake technology have transformed digital governance through the creation of remarkably realistic synthetic audio, video and image content. These technologies can apply to education, healthcare, entertainment, governance, and business, but they also create difficult legal and constitutional questions. There has been a noticeable increase in the misuse of deepfakes for furthering misinformation, influencing election results, obtaining money through deception, identity theft, cyberbullying, and creation of non-consensual intimate imagery. Indian law as it stands primarily consists of the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Bharatiya Nyaya Sanhita,

[7] INDIA CONST. arts. 14, 19 & 21; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)
[8] Information Technology Act, No. 21 of 2000, INDIA CODE (2000); Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 25, 2021).
[9] High-Level Expert Group on Artificial Intelligence, European Commission, Ethics Guidelines for Trustworthy AI (2019); OECD, OECD Principles on Artificial Intelligence (2019); UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

2023, and the Digital Personal Data Protection Act, 2023.[10] However, these laws were not originally made to regulate involve AI-generated synthetic media or deepfakes in a comprehensive manner.

Thus, this paper is based on the following research questions.

1. What are the legal challenges presented by deepfakes and generative AI in India?
2. Is the existing legal framework sufficient to regulate AI-generated synthetic media in India or is there a huge gap?
3. In what way do deepfakes impede the rights guaranteed under the Constitution of India - relating to privacy, dignity, equality, reputation and freedom of speech and expression?
4. What regulatory lessons can India learn from international frameworks, such as the European Union's AI Act and other risk-based AI governance models?
5. Shouldn't there be a specific legislation in India to govern deepfakes, algorithmic accountability, transparency obligations, and civil liability in Artificial Intelligence?
6. What constitutional safeguards and principles of governance ought to underlie the future AI regulatory framework for India? How could these processes ensure the protection of the country's democracy and fundamental rights?

D. Research Hypothesis

The hypothesis of this research is that the advent of deepfakes and Generative AI has outstripped the evolution of law and the Constitution in India. Current laws primarily focus on cybercrimes after the fact and do not have specific provisions for the creation, dissemination, authentication, liability and regulation of AI-created synthetic content.[11] Moreover, the evolution of constitutional law that addresses privacy and

[10] Information Technology Act, No. 21 of 2000, INDIA CODE (2000); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021); Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).

[11] Ministry of Electronics & Information Technology, Government of India, *India AI Governance Guidelines* (5 November 2025). The 2024 Advisory Group Report may be retained only as background material, but the 2025 Guidelines should be cited as the current national AI-governance framework.

dignity, free speech, and informational autonomy has occurred mainly in the context of conventional digital technologies. In light of these, the research gives the following hypothesis.[12]

India's present legal and institutional framework has evolved through the *India AI Governance Guidelines* released by MeitY on 5 November 2025, which set out a principle-based and techno-legal framework for safe, responsible and inclusive AI governance. However, the framework primarily adapts existing legal instruments such as the IT Act, the DPDP Act and the BNS, rather than creating a standalone AI statute. Accordingly, while the Guidelines strengthen India's policy response through seven guiding "sutras," an AI Governance Group, a Technology & Policy Expert Committee and related institutional mechanisms, they do not fully resolve the need for binding AI-specific obligations on risk classification, audits, liability allocation and remedies for deepfake-related harms.

The purpose of Reading down, Judicial interpretation and Evolution-based on Efficiency of Article 21 of the Constitution asked for the present-day modifications of Article 21. The capacity act also needs purposive reading down to ensure better regulation of technology.

E. Research Methodology

The doctrinal legal research method is being adopted in the present study to analyses the upcoming legal and constitutional issues that deepfake and generative artificial intelligence (AI) may face in India. Due to the research being mainly about a statutory interpretation, constitutional principles, judicial precedents, and comparative regulatory models, a doctrinal approach would be the most appropriate methodology for assessing the adequacy of current legal regime and suggesting normative reforms.

The nature of the research is analytical and descriptive. The evolution of generative AI technologies and deepfake applications have shown definite evidence that they

[12] K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India); Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India); Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1 (India).

would have tremendous implications for privacy, misinformation, electoral integrity, intellectual property, and democratic governance.

The analytical section examines the effectiveness of the existing legal framework in India, namely, the Constitution of India, the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, at addressing AI-generated harms. In order to identify best practices that can be adapted to the Indian legal context, the study employs a comparative approach, examining international regulatory developments, including the European Union AI Act, the UNESCO Recommendation on the Ethics of Artificial Intelligence[13], the OECD AI Principles, and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.

The research work is based on both primary and secondary sources. The constitution, laws passed by the Parliament, laws made by delegated legislation, judgements of the Supreme Court and various High Courts, Parliamentary Standing Committee, MeitY's advice on AI, and the government's own policies on digital India serve as Primary sources.

Constitutional landmark rulings examined include *Justice K.S. Puttaswamy v. Union of India*, *Shreya Singhal v. Union of India*, *Anuradha Bhasin v. Union of India*, and *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, which together illuminate the constitutional protection of privacy, freedom of speech, due process and proportionality.

The secondary sources will include books, peer-reviewed journal articles indexed in Scopus and Web of Science, Law Commission reports, white papers of the government, international policy documents, OECD reports, UNESCO ethical guidelines, comparative legal scholarship, the writings of leading scholars, and other academic writings of Stuart Russell, Luciano Floridi, Ryan Calo, Cary Coglianese, Danielle Citron, Bobby Chesney, Karen Yeung, Jack Balkin, Julie Cohen, etc.

[13] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

F. Review Of Literature

The department of information technology has accelerated their engagement in digital marketing and e-commerce activities. A need has arisen for educational programs. Out of all innovations this deepfakes is one of the most disruptive technologies it blurs the line between real and fake digital content. Although there are enormous opportunities for growth in the economy, governance, health, education, etc., arising out of artificial intelligence (AI), it also poses unprecedented legal and constitutional challenges in areas of privacy, dignity, freedom of speech and expression, electoral interference, cybercrime, democratic accountability, etc. The topics have been studied from different disciplines as per literature; however, a legal scholarship which comprehensively links constitutional governance with regulation of AI in the Indian context is relatively sparse.

1. Supervision of AI

The foundational work of Stuart Russell and Peter Norvig was important in laying the groundwork of the literature on artificial intelligence governance. The book Artificial Intelligence: A Modern Approach considers an AI to be a system that creates rational actions. However, it is vital that we align machine behavior with human values. The technological foundation for comprehending generative AI is provided by their work, but constitutional regulation or democratic accountability receives comparatively limited attention.

Luciano Floridi makes a major contribution to AI governance scholarship by arguing that AI should be governed in the infosphere, and these governance principles should be transparent, accountable, fair, and explainable.[14] Floridi recommends the creation of risk-based regulatory frameworks that combine ethical standards with legal accountability. His contribution has had a significant impact on the UNESCO's Recommendation on the Ethics of AI, and the EU AI Act. In the same way, Ryan Calo studies AI from the perspective of law and public policy and argues that existing legal

[14] Luciano Floridi, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities, 21 Minds & Mach. 689 (2019).

doctrines simply aren't up to the task of autonomous systems creating unexpected harms.[15]

According to him AI governance cannot be settled with legislation but needs continuous monitoring, adaptive regulation, algorithmic accountability and regulatory experimentation. Cary Coglianese presents evidence-based regulatory frameworks using technology and the principles of administrative law.[16] He argues for implementation of models by regulators which are adaptable and risk sensitive which will keep evolving. His scholarship is invaluable to the conversation regarding regulatory agencies and AI governance.

2. Regulating Deepfakes

Deepfakes pose a serious threat to both democracy and national security. Most important, they are also a threat to privacy and personal dignity.[17] Two of the leading scholars in law who have written on deepfakes are Danielle Keats Citron and Bobby Chesney. They recognize various types of harm. For example, non-consensual intimate imagery, political misinformation, financial fraud, identity theft damage to reputation. Significantly, they contend that existing legal remedies such as defamation and privacy law are insufficient, as they only function post-harm.

Danielle Citron advances the idea of "cyber civil rights" and argues for legal protections against technologically enabled abuse.[18] She points out that the digital editing of images has a differential impact on women, journalists, political candidates, and marginalized groups, requiring specialized statutory protections rather than generalized tort law. In the following years, scholars started looking into the capacity of online intermediaries to prevent the transmission of deepfakes. This would happen through content moderation, algorithmic detection, and platform accountability.

[15] Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399 (2017).
[16] Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147 (2017).
[17] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019).
[18] Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (2022)

Experts increasingly endorse a mix of criminal sanctions, civil remedies, watermarking technologies, provenance authentication and mandatory disclosure obligations for AI-generated content. Nonetheless, most of this literature focus on the US and The European Union, which leaves considerable scope for an analysis of the intermediary liability framework in India under the Information Technology Act and Information Technology Rules, 2021.

3. Digital Constitutionalism

A growing body of scholarship reconceptualizes digital governance as digital constitutionalism, which seeks the preservation of constitutional values in digitally mediated societies. According to Karen Yeung, the automated processes enabled by algorithmic governance alter the interactions between the citizenry and the State, with potentially adverse consequences for transparency, accountability and procedural fairness.[19]

Her argument is that the constitutional safeguards have to keep pace with the way algorithmic power is exercised by the State and technology companies. Jack Balkin coined the term information fiduciary, because he believes that digital platforms have substantial informational power over users; therefore, these platforms owe duties similar to fiduciary duties.[20] According to Balkin, digital platforms must be regulated due to their de facto monopoly and resulting harm to society. In the same vein, Julie Cohen laments the concentration of informational power within digital ecosystems and advocates for governance models that are premised on human agency, democratic participation and informational self-determination.[21]

D. Constitutional Jurisprudence in India.

The Constitution of India provides an important normative framework to regulate generative AI and deepfakes. A case from 2017 where Supreme Court of India upheld the right to privacy. This ruling is what gives rise for the regulation of unauthorized AI-generated content that uses personal identity and biometric data. The verdict

[19] Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Reg. & Governance 505 (2018).
[20] Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183 (2016).
[21] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (2019).

passed by The Kerala High Court in *Faheema Shirin R.K. v. State of Kerala*, W.P.(C) No. 19716 of 2019, recognised the relevance of internet access to constitutional freedoms under Articles 19 and 21. Until the SCC OnLine citation is confirmed from the official reporter database, the writ-petition number, decision date and AIR parallel citation may be used to avoid reliance on a disputed reporter number.[22] Although artificial intelligence (AI) was not directly addressed, this judgment illustrates how the judiciary is understanding digital rights and constitutional protections.

IV. RESEARCH & ANALYSIS

A. Evolution of Deepfakes and Generative AI: Conceptual and Technological Foundations

The fast-evolving nature of AI is transforming the digital world. It enables machines to create, alter and interpret information with remarkable accuracy. Among the most disruptive innovations in this area that have changed digitalification ofcommunication, creativity, and information dissemination are Generative Artificial Intelligence (Generative AI) and deepfake. Generative AI refers to machine learning systems that create new content such as text, images, videos, audio, computer code, and synthetic datasets.

While they can broadly refer to any type of generative model, deepfakes are a very specific application of generative models that create a highly realistic-looking but synthetic audio-visual representation of someone. The coming together of these technologies has brought significant economic and social opportunities but posed serious constitutional, legal and ethical issues. To understand the origin of Generative AI, one must look towards machine learning and the artificial neural networks modelled after the human brain, which all helped the technology come to fruition.

During the early days, AI systems relied on rule-based programming, which specified how to compute. With the advent of deep learning in the early 2010s, AI development was transformed as machines began learning patterns from masses of data as opposed

[22] *Faheema Shirin R.K. v. State of Kerala*, W.P.(C) No. 19716 of 2019 (Ker. H.C., decided 19 September 2019), also reported as AIR 2020 Ker 35. The SCC OnLine citation should be verified directly from SCC OnLine before final submission, as secondary sources conflict between "2019 SCC OnLine Ker 1733" and "2019 SCC OnLine Ker 2976."

to mere sets of rules.[23] The deep neural networks, particularly convolution neural networks (CNNs) and recurrent neural networks (RNNs), paved the path for modern generative models which produce more and more complex synthetic outputs. Later advancements sped up generative power.

VAEs, diffusion models, and, more recently, transformer-based large language models (LLMs) have significantly improved the quality, scalability, and accessibility of generative AI. New AI systems like OpenAI's GPT series, Google's Gemini, Anthropic's Claude and image-generation models like DALL·E, Midjourney and Stable Diffusion show that generative technology is no longer an academic lab product, but one that's commercially available to millions across the globe. As a result, the ability to fabricate realistic synthetic media no longer requires technical know-how and increases misuse.

The earliest deepfakes were experimental applications applied in computer vision research that manipulated faces and images. Improvements made in facial recognition, motion capture, voice cloning, and natural language processing have resulted in the creation of complete synthetic identities that can simulate the facial expressions, voice, gestures, and mannerisms of real individuals. Today's deepfake technology allows the generation of these videos of public figures or celebrities – such as a politician mimicking speech or endorsing product, or even a non-celebrity in an intimate act. The advanced technology has made it difficult for people to differentiate between real and fake digital evidence. Scholars refer to this situation as the "liar's dividend." At present, even real evidence may be disregarded as being fake. Generative AI is also used in beneficial domains such as drug discovery, medical imaging and personalised treatment planning in healthcare.[24]

Educational institutions are increasingly coming up with AI-powered systems that offer tailored learning. The entertainment field utilizes synthetic media for still and motion pictures, multilingual dubbing, archival restoration of historical assets, and virtual production. The use of generative systems for customer service, software

[23] Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach 22–39 (4th ed. 2021).
[24] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753, 1765–68 (2019).

development, legal research, document automation, and more enhances productivity across businesses.[25]

B. Constitutional Implications of Deepfakes in India (Articles 14, 19 & 21)

The emergence of deepfakes and Generative Artificial Intelligence (AI) raises potential constitutional issues in India. They challenge the guarantees of equality before the law and equal protection of the law, freedom of speech and expression, and the right to life and personal liberty under articles 14, 19, and 21 of the Constitution. While the Constitution was written decades before digital technology, it is dynamic enough for the courts to interpret it in light of contemporary technology.

The unprecedented ability of Generative AI to tamper with information, create identities and distort public discourse gives rise to doubts as to whether current constitutional doctrines are equipped to deal with algorithmic harm. As a result, the constitutional debate is not just about technology regulation; it also encompasses an array of issues such as the preservation of democracy, dignity, and the rule of law.

C. Law and Algorithmic Fairness: Article 14.

Article 14 provides for equality before the law and equal protection of the laws. It prohibits arbitrary action by the State and requires the State to act fairly and reasonably.[26] Article 14 has normally been used to strike down discriminatory legislation and executive action. Nonetheless, as public authorities increasingly deploy AI systems, a new dimension to constitutional equality is of strategy is the issue of algorithmic discrimination. Generative AI systems are often trained on giant datasets that still carry historical discrimination related to gender, caste, religion, ethnicity, language, and socioeconomic status.

Therefore, human influence will be required to eliminate any unintended consequences. The situation is made even more complicated by deepfake technologies, which can be used for selective impersonation, political misinformation and the targeting of women, minorities, journalists and political opponents. The constitutionally guaranteed substantive equality enshrined in Article 14 is violated by

[25] UNESCO, Guidance for Generative AI in Education and Research 8–20 (2023).
[26] INDIA CONST. art. 14.

such discriminatory impacts. Article 14 has been interpreted by the Supreme Court to mean prohibition of arbitrariness in the action of the State.

The Court famously ruled in E.P. Royappa v. State of Tamil Nadu that arbitrariness is the antithesis of equality.[27] In today's digital era, the principle assumes renewed importance as the opacity of algorithmic decision-making could lead to potentially arbitrary outcomes that are not explained nor held accountable in any meaningful way. AI-enabled systems used by governmental agencies for surveillance, welfare, law enforcement or predictive policing must be reasonable and transparent as per Article 14.

D. Article 19(1)(a): Freedom of Speech and Expression v/s Harmful Synthetic Media

As per Article 19(1)(a) the fundamental right of freedom of speech and expression includes the right to artistic creativity, political speech and communication, academic work and access to information.[28] Generative AI opens up avenues for expressive potential that weren't possible before, by enabling content creation and driving innovation across domains. More and more writers, artists, educators, and researchers are using AI-powered tools to enhance creativity. Article 19(1)(a)'s constitutional protection is not absolute, however.

The provision 19(2) permit reasonable restrictions in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, decency, morality; contempt of court; defamation; incitement to an offence; and integrity of the judicial proceedings.[29] Deepfakes are often based on one or more of these grounds: defamatory speech, election misinformation, communal incitement, market manipulation, and reputational harm. The constitutionality issue is delineating beneficial AI-generated expression from harmful deepfakes. Imposing overly stringent rules may hamper innovation as well as legitimate political expression, while applying none could weaken democracy itself.

[27] E.P. Royappa v. State of Tamil Nadu, (1974) 4 S.C.C. 3
[28] INDIA CONST. art. 19(1)(a).
[29] INDIA CONST. art. 19(2).

The Supreme Court ruling Shreya Singhal v. Union of India[30] is very useful for constitutional interpretation in this regard. The court while striking down section 66A of Information Technology (IT) Act, 2000 said that restrictions on online speech must meet the constitutional standard of reasonableness and cannot be vague or overbroad. As such, any future laws that might regulate deepfakes should focus on defining the prohibited act rather than banning all AI-generated content. Likewise, direct access to digital communication platforms is an integral part of contemporary freedom of expression, as noted in Anuradha Bhasin v. Union of India by the Supreme Court.

In a world where AI-generated communications are increasingly becoming part of the digital ecosystem, the regulatory interventions concerning Generative AI must pass the constitutional tests of necessity, proportionality, and procedural safeguards.

E. Privacy, dignity, reputation and informational autonomy - Art. 21

The most serious constitutional implications of deepfakes stems from Article 21, which states that no person shall be deprived of his life and personal liberty, except by a procedure established by law.[31] The ambit of Article 21 has been expanded by judicial interpretation to include the right to life, dignity, privacy, autonomy, reputation, informational self-determination and protection from arbitrary State actions.

The Supreme Court verdict in Justice KS Puttaswamy (Retd.) v Union of India held that a person has a right to privacy which is a fundamental right.[32] The Court highlighted that privacy of information permits one to exercise objective and meaningful control over the collection, processing, dissemination and use of data. Deepfake techs violate the constitution by accessing a person's facial features, voice, biological features, identity, and more, without their permission. Deepfakes allow people to create wholly fake conduct associated with innocent victims unlike traditional identity theft. Victims suffer severe psychological, professional and reputational harm.

[30] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.
[31] INDIA CONST. art. 21.
[32] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

The creation of sexually explicit deepfakes without consent constitutes a serious violation of bodily autonomy, dignity and privacy, and women are disproportionately affected. Such new content is often removed but causes permanent reputational damage to people. As a result, an individual's identity and information are also protected under Article 21. The Supreme Court has recognized that reputation is an essential element of the right to life under Article 21.[33]

F. Balancing the Constitution and Necessitating Rights-based AI Governance.

Regulating generative AI as per the Constitution requires balancing two set of competing Fundamental Rights without prioritizing tech or regulatory. The Supreme Court has repeated endorsement of propaganda and proportionality offers an apt constitutional framework to evaluate future AI law.[34] Policies regarding AI-generated content must be aimed at a legitimate government purpose, necessary to accomplish that purpose, the least restrictive means available to achieve that purpose, and may not unduly burden individual rights and interests.

As Generative AI changes the way we communicate, we need constitutional jurisprudence to evolve so that technology doesn't become incompatible with the basic structure of the Constitution of India.

G. Existing Legal Framework Governing AI and Deepfakes (Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, Bharatiya Nyaya Sanhita, 2023, Copyright Act, 1957, Information Technology Rules, 2021, and Allied Regulatory Framework)

The IT Act is the primary legislation on cyberspace in India. It was enacted in 2000 and is called the Information Technology Act. The Act, which was mainly brought into effect to facilitate electronic commerce and to recognize digital signatures, has many provisions that address harms from deep fakes and AI-generated content. Section 66D makes it an offence to cheat by personation through the use of computer resources.[35] There will be particular relevance to the section where deepfakes are used.

[33] Subramanian Swamy v. Union of India, (2016) 7 S.C.C. 221.
[34] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 S.C.C. 353; Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1.
[35] Information Technology Act, No. 21 of 2000, S. 66D, India Code (2000).

For example, impersonating a public official, celebrity, financial institution or private individual to cheat."

Voice cloning through AI and artificially created video calls are increasingly used for cyber fraud, phishing, investment scams and impersonation. This may give rise to liability under this provision. The publication or transmission of obscenity, sexually explicit, and child sexual abuse material in electronic form is prohibited under sections 67, 67A, and 67B. Due to the rampant usage of non-consensual intimate deepfakes of women and minors, these provisions are crucial. Even though the statutory language was drafted prior to synthetic media, the courts may interpret these provisions broadly in view of AI-generated explicit content where the resulting harm is still substantially similar to conventional digital exploitation. According to Section 69A of the IT Act, the Central Government has the power to block public access to online information in certain circumstances.

H. The Digital Personal Data Protection Act, 2023, read with the Digital Personal Data Protection Rules, 2025, is India's principal legal framework for the processing of digital personal data

Although the framework does not specifically target Generative AI, it is highly relevant because many AI systems depend on large personal datasets for training, deployment and continuous improvement.[36] Facial images, voice samples, biometric identifiers and other identifiable data may be collected or processed without the knowledge or consent of the data principal and then used to create synthetic media. The DPDP Act recognises consent as a central basis for lawful processing and imposes obligations on data fiduciaries relating to purpose limitation, data minimisation, accuracy, security safeguards and accountability.

The DPDP Rules, 2025 further operationalise this framework through mechanisms such as Consent Managers, personal-data breach notification, verifiable parental consent for children's data, and additional compliance obligations for Significant Data Fiduciaries, including Data Protection Impact Assessments and audits[37]. These mechanisms may strengthen control over the collection and processing of personal

[36] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

data used in deepfake creation. Victims may also rely on rights relating to access, correction, erasure, nomination and grievance redressal. However, the DPDP framework remains limited in the context of Generative AI because it regulates personal-data processing rather than AI-generated outputs as such.

Once a deepfake is generated and disseminated, the framework offers limited direct remedies for reputational injury, misinformation or synthetic impersonation. Accordingly, even after the DPDP Rules, 2025, the regime strengthens informational privacy but cannot be treated as a complete AI-governance framework.

I. The Bharatiya Nyaya Sanhita, 2023, which came into force on 1 July 2024, has replaced the Indian Penal Code, 1860, except for the deferred provision under Section 106(2)

The BNS contains provisions that can be invoked against the misuse of deepfake technology for malicious purposes. Although the BNS does not expressly refer to Artificial Intelligence[38], many of its offences are sufficiently technology-neutral to cover AI-generated criminal conduct. Deepfakes may attract criminal liability for cheating, forgery, criminal intimidation, identity-related deception, defamation, extortion, publication of obscene material, and offences against women.

Fabricated videos of public officials accepting bribes, fake financial documents created with AI, or synthetic voice recordings enabling cyber frauds could fulfil the essential elements of cheating and forgery offences. Similarly, deepfakes with sexual content which target women may amount to offences affecting modesty, privacy or sexual dignity under the BNS in addition to the corresponding provisions of the IT Act.

The Copyright Act, 1957 is becoming more and more relevant as Generative AI systems produce various works like literary works, artworks, music, software, and audio-visuals by using copyrighted materials for their training.[39] There are two separate legal problems concerning deepfakes. The first pertains to the unlawful use of copyright material to train a model. Holders of rights are increasingly stating that

[38] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).
[39] Copyright Act, No. 14 of 1957, India Code (1957).

scraping copyrighted content on a large scale without authorisation breaches their exclusive statutory rights.

At present, Indian copyright law does not contain an explicit exception for datasets used to train AI, which creates complications regarding legal uncertainty over fair dealing and permissible use through computation. The second point is that deepfakes use the performance, voice, image, video or art of an identifiable person.

J. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in relation to synthetically generated information, now constitute one of India's most direct regulatory responses to deepfakes

The Rules continue to prescribe intermediary due diligence, grievance redressal, removal of unlawful content on actual knowledge, cooperation with government agencies, preservation of records, and additional compliance obligations for Significant Social Media Intermediaries. Importantly, the 2026 amendment introduced a statutory definition of "synthetically generated information" under Rule 2(1)(wa), covering artificially or algorithmically created, generated, modified or altered audio-visual information that appears real, authentic or true.[40]

Rule 3(3) further requires intermediaries that enable the creation, publication, transmission, sharing or dissemination of such information to deploy reasonable and appropriate technical measures, including automated tools, to prevent unlawful SGI.[41] It also requires lawful SGI to be clearly and prominently labelled and embedded, to the extent technically feasible, with permanent metadata or other provenance mechanisms, including a unique identifier.

These obligations mark a significant shift from advisory-based governance to binding due-diligence standards. However, the amendment remains limited because it does not fully resolve questions of attribution, liability allocation among developers,

[40] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021).
[41] Ministry of Electronics & Information Technology, Government of India, Advisory to Intermediaries and AI Platforms on Due Diligence Obligations Under the IT Rules, 2021 (Mar. 1, 2024).

deployers and users, independent audits, false positives in automated detection, or remedies for victims after harmful deepfakes have already circulated.

K. There remains a need for comprehensive AI legislation despite the SGI-focused amendment to the IT Rules

India's framework is no longer entirely silent on deepfakes, since the amended IT Rules now impose labelling, metadata, provenance and technical-measure obligations on intermediaries dealing with synthetically generated information. Nevertheless, these rules address only selected aspects of synthetic-media governance and do not regulate the entire AI lifecycle. India still requires clearer statutory provisions on algorithmic impact assessments, independent AI audits, transparency obligations, risk-based classification of AI systems, explainability, human oversight, and the allocation of liability among AI developers, deployers, intermediaries and users. The transnational character of AI development also complicates enforcement because many generative AI models are developed outside India while their outputs are instantly disseminated through globally accessible digital platforms.

L. Comparative Legal Analysis: Lessons from the European Union, United Kingdom, United States, China, Singapore, and Other Jurisdictions

1. European Union: The AI Act and Rights-Based Governance Framework

The worldwide leader in AI regulation has become the EU with the adoption of the Artificial Intelligence Act (AI Act), the world's first comprehensive horizontal legislation on AI systems. Unlike other, traditional technology-neutral statutes, the AI Act defines and regulates AI technologies in a risk-based manner and allocates various AI applications to various risk levels that affects the fundamental rights, public safety as well as democratic institutions.[42]

The law of AI classifies AI systems as unacceptable-risk AI, high-risk AI, limited-risk AI and minimal-risk AI. AI systems that pose unacceptable risks including certain forms of manipulative AI, exploitative systems and prohibited biometric practices will be prohibited. High-risk systems used in sectors such as health, policing, education,

[42] Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).

employment, migration, and critical infrastructure will have stringent obligations relating to risk assessment, transparency, human oversight, cybersecurity, data governance and conformity assessments before being placed on the market. Regulations in United Kingdom: Principles Based and Innovative.

The UK has chosen a decentralized sector-specific regulatory approach unlike the European Union. The UK Government's AI Regulation White Paper (2023) does not propose a full AI law but rather a pro-innovation framework based on five cross-sector principles: safety, transparency, fairness, accountability and contestability. The ICO, CMA, FCA, and Ofcom will have to apply these principles in respect of their regulation of relevant economic sectors.[43]

This flexible approach aims to avoid overregulation but promote innovation and investment in AI. Nonetheless, there are critics who would say a lack of legally binding obligations may lead to inconsistent regulatory approaches and uncertainty in law enforcement, especially in relation to deepfake technologies and algorithmic accountability. Still, the UK's focus on adaptive governance and regulatory coordination can offer useful lessons for India, where several sectoral regulators already have overlapping jurisdiction over digital technologies.

2. Sectoral Regulation and Emerging Deepfake Legislations-United States

Currently, the U.S. does not have an overarching federal AI law that's similar to the EU AI Act. AI governance is shaped by federal executive initiatives, sector-specific regulation, state legislation, consumer protection law, and the development of judicial precedents. Federal government agencies like the Federal Trade Commission (FTC) are turning to existing statutes in order to tackle misleading AI, biased algorithms and unlawful business practices.[44] Moreover, executive activities have emphasized responsible artificial intelligence advancement, encryption, transparency and safeguarding of civil rights in automated choices.

[43] Dep't for Sci., Innovation & Tech., A Pro-Innovation Approach to AI Regulation (White Paper, 2023).

[44] Federal Trade Commission, Keep Your AI Claims in Check (Feb. 2023); Federal Trade Commission Act, 15 U.S.C. ss 41–58.

3. Comparative Approach Lessons

Even with sizeable jurisdictional disparities, there are a number of similarities. The growing acknowledgment in various jurisdictions that deepfakes pose different regulatory challenges requiring some kind of legal response and not just traditional cybercrime ones. Transparency obligations are also a key means of resisting muzzling mis- and disinformation, be it through mandatory labelling or watermarking of content generated by AI.

Third, regulatory regimes increasingly promote risk-based governance assigning additional due diligence and other obligations to AI systems that can affect the fundamental rights, elections, healthcare, criminal justice, financial markets, or public administration.

Fourthly, the overwhelming majority of the jurisdictions recognize that the institutional accountability is required for AI governance not only amongst end-users. But also extends to developers, deployers, distributors and digital intermediaries.

For India, the European Union's rights-based approach seems to fit well within the existing constitutional framework produced by Articles 14, 19, and 21. At the same time, the United Kingdom's adaptive regulatory principles, Singapore's emphasis on ethical governance, and China's technological safeguards present useful policy tools that can be selectively assimilated without compromising constitutional freedoms. As such, India should not replicate any foreign model in totality.

M. Challenges in Regulating Deepfakes and Generative AI

1. Lack of a Broad Regulatory Framework for AI

The main challenge is that there is no existing law focused only on Artificial Intelligence and synthetic media. Legislation in force such as Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; Bharatiya Nyaya Sanhita, 2023; Copyright Act, 1957, etc. tackle the misuses of AI for the most part without regulating the life cycle of AI.[45] Primarily geared towards electronic transactions, cybercrime,

[45] Information Technology Act, No. 21 of 2000, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023); Copyright Act, No. 14 of 1957, India Code (1957).

data protection, and intellectual property, these statutes do not mention algorithmic governance.

Thus, they lack provisions on risk classification, mandatory algorithmic audits, explainability, transparency, human oversight, and accountability of AI developers and deployers. The resulting fragmentation of the law has created uncertainty for regulators, tech companies, courts and victims. Often, an injured person will have to rely on the multiple statutory remedies at their disposal simultaneously. On other hand, enforcement agencies need to grapple with identifying the precise violation as per the respective framework on the AI generated harm.

2. Challenges in Attribution and Criminal Investigation

Deepfakes are often further obscured from their creators of traditional cyber offences through anonymization technologies, encrypted communications, VPNs, and blockchain or other distributed digital infrastructures. Generative AI models being increasingly capable of generating synthetic output on their own accord based on user prompts has further complicated legal attribution. One of the most significant unresolved questions in AI governance is who, if anyone, is liable for the use of an AI system: the software developer, the model provider, the platform operator, the content creator, or the end user? Generative AI use multiple participants at various stages of algorithmic construction and deployment. Existing criminal law mainly operates on a presumption of direct human agency. The investigation and prosecution may nonetheless be rendered ineffective in the absence of clear statutory allocation of responsibility.

3. The Constitution: Free Speech vs. Preventing Harm

Regulating deepfakes will have to balance competing constitutional values. Malicious synthetic media can further fraud, election interference, hate speech, defamation, financial crime, and gender-based violence. Overregulation, however, may undermine the freedom of speech and expression guaranteed by Article 19(1)(a) of the Constitution.[46] Generative AI does not cause harm. It backs legitimate artistic creation, education, scientific research, journalism, accessibility for handicapped persons,

[46] INDIA CONST. art. 19(1)(a), art. 19(2).

software development and public administration. The imposition of broad prohibitions on the use of A.I. Technology by law may impact innovation and democratic discourse that may stifle growth.

4. Technology is rapidly evolving and regulations are not

Artificial intelligence is advancing much faster than lawmakers can develop regulations. Continuous development of new generative models associated with voice cloning, multilingual, image, autonomous agents, and video generation is sharpening their capability. Laws in place for one generation of AI technology may be outdated by the time they are used. As is often the case with technology law, regulatory adaptation never catches up with the innovation.[47] Legislative approaches that are static are unlikely to work against ever-evolving AI architectures. As a result, regulatory frameworks, where appropriate, must be technologically neutral while including adaptation mechanisms that enable periodic revision, technical standards and delegated rule-making.

5. Governance of Platforms and Jurisdiction Beyond Borders

Due to the global architecture of digital platforms, significant jurisdictional issues arise. AI systems are often developed outside of India, with cloud hosting being done on foreign infrastructure, they are trained on datasets sourced globally and on-boarded by multinational technology. Harmful deepfake content may thus be created in one jurisdiction, target victims in another, and be circulated around the world in minutes. these transnational realities pose a challenge to the existing standards of territorial jurisdiction.

Due to the different national regulatory frameworks in the area of privacy, intermediary liability, freedom of expression and criminal jurisdiction, international cooperation becomes more complicated. To enforce this effectively requires strengthened the mutual legal assistance framework, harmonized standards of digital evidence and better cooperation between regulatory authorities of different jurisdictions.

[47] Gary E. Marchant, Braden R. Allenby & Joseph R. Herkert, The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight 19–35 (2011)

6. Gendered Harm, Electoral Integrity, and Public Trust

The relationship between electoral integrity and public trust in the context of gendered harm. Deepfakes impact women, journalists, candidates, public figures at higher rates. Generative Artificial Intelligence is deployed to create a new wave of non-consensual sexually explicit synthetic content. Such content is particularly harmful because it inflicts substantial psychological harm, hurts reputations, and other violations. Most legal remedies remain essentially reactive, post-publication, making harms irreversible before relief is offered. Likewise, false AI-generated material may disrupt elections. Hence, AI-generated false speeches, fake campaign ads, and synthetic endorsements could skew public opinion during elections. Content of that sort can hamper informed political participation and weaken confidence in democracy.[48]

7. Institutional Ability and Regulatory Coordination

AI governance must be institutionalized and expertise must become a priority. Judges, police authorities, prosecutors, regulators, forensic labs, and administrative agencies need training on new AI technologies, algorithm functioning, digital evidence, and synthetic media detection.

V. SUGGESTIONS AND RECOMMENDATIONS

The swift evolution of deepfake and generative AI technology has revealed continuing shortcomings in India's regulatory framework, even after recent reforms. India should move toward a rights-based and technologically adaptive AI governance regime that builds upon, rather than overlooks, the SGI-related amendment to the IT Rules, 2021. That amendment has already introduced important obligations concerning labelling, metadata, provenance and technical measures for synthetically generated information. However, it does not amount to a complete AI statute.

A comprehensive AI-specific law should define deepfakes, synthetic media and generative AI systems, while clearly identifying the responsibilities of developers, deployers, intermediaries and end-users. Existing responses under the IT Act, 2000,

[48] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753, 1779–81

the DPDP Act, 2023, the Bharatiya Nyaya Sanhita, 2023 and the amended IT Rules provide partial remedies, but they do not fully address algorithmic accountability, risk assessment, independent audits, liability allocation, victim compensation and cross-border enforcement. Instead of treating watermarking as an unaddressed proposal, future reform should strengthen the existing labelling and provenance framework by making it technically robust, auditable and enforceable.

India should also consider an independent Artificial Intelligence Regulatory Authority or coordinated institutional mechanism to certify high-risk AI systems, issue binding standards, conduct compliance audits, investigate AI-related violations and coordinate with CERT-In, the Data Protection Board and law-enforcement agencies.

Accountability of Platforms Should be Strengthened Both AI service providers and social media intermediaries must be legally required to deploy proactive detection technologies, quick grievance redressal, transparency in content moderation policies and removal of verified harmful deepfake content. The conditionality of safe-harbour protection should be dependent on the compliance of statutory due diligence obligations. Strengthen Victim centric Legal Remedies.

The procedures to obtain interim injunctions, blocking orders, compensation and removal of harmful synthetic media should be fast tracked. It becomes crucial to protect women, children, public figures, journalists, and other vulnerable communities against deepfake abuse, including the creation of non-consensual intimate imagery and identity theft. India must invest heavily in infrastructure and forensic capabilities for AI detection.

It is recommended to set up forensic laboratories at national and state levels that have sophisticated AI detection tools. Officers of law enforcement, prosecution and judiciary should be regularly trained for preservation of digital evidence generation of artificial intelligence content and cyber forensic investigation for effective enforcement. The last one, there is a need to have more public awareness and digital literacy programmes in place across the country. There ought to be collaborations among educational institutions, civil society organisations and IT companies, to help citizens identify deepfakes, verify digital content, protect personal information and

 (ISSN: 2583-7753)

use generative AI technology responsibly. Digital literacy must be a part of the schools and university curricula. Lastly, international cooperation is crucial given the transnational character of AI platforms.

India must join global norms clashing regarding AI Governance, help in cross border offences investigation, ensure national regulation align with global norms requirements of transparency, human oversight accountability and fundamental rights. This collaboration will aid India in ensuring responsible artificial intelligence innovation and digital governance.

VI. CONCLUSION

Generative Artificial Intelligence (GAI) is a set of artificial intelligence methods, tools, and resources through which a computer generates or suggests digital objects such as sound, images, and texts based on user prompts. Even though India has made important legal moves through the IT Act, 2000, Digital Personal Data Protection Act, 2023, and Bharatiya Nyaya Sanhita, 2023, yet the existing legal framework is fragmented and inadequate to tackle the complex issues stemming from rapidly evolving AI technologies. Based on this research, deepfake regulations cannot be contouring merely through traditional cybercrime laws or intermediary liability frameworks. An integrated legal framework based on values of constitution is required.

A framework must protect the fundamental rights to privacy, freedom of expression, equality and due process while ensuring that technology does not get unjustifiably hindered. The responsible governance of AI necessitates transparency, accountability, human mapping as well as effective remedies for victims of AI. India aspires global leadership in AI but if depends technology advancement and a robust regulation regime that is trustworthy.

With AI-specific law, watermarking standards, stronger platform accountability, dedicated regulatory institutions, advanced forensic capacities, and greater digital literacy for the public, the country can better protect itself against malicious synthetic media. In conclusion, deepfakes' challenge is not just technological but also constitutional and sociological. The digital governance future consists of a legal

regime that fosters innovation while safeguarding democratic institutions and individual rights and ensuring public trust in digital communications. The need of the hour for India to mitigate the risks but tap into the benefits of generative AI is a proactive, adaptable, human-centric regulatory framework.

VII. REFERENCES

1. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
2. Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).
3. Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147 (2017).
4. Copyright Act, No. 14 of 1957, India Code (1957).
5. Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (2022).
6. Dep't for Sci., Innovation & Tech., A Pro-Innovation Approach to AI Regulation (White Paper, 2023).
7. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
8. E.P. Royappa v. State of Tamil Nadu, (1974) 4 S.C.C. 3.
9. *Faheema Shirin R.K. v. State of Kerala*, W.P.(C) No. 19716 of 2019 (Ker. H.C., decided 19 September 2019), also reported as AIR 2020 Ker 35. The SCC OnLine citation should be verified directly from SCC OnLine before final submission, as secondary sources conflict between "2019 SCC OnLine Ker 1733" and "2019 SCC OnLine Ker 2976.
10. Federal Trade Commission, Keep Your AI Claims in Check (Feb. 2023); Federal Trade Commission Act, 15 U.S.C. ss 41–58.
11. Gary E. Marchant, Braden R. Allenby & Joseph R. Herkert, The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight 19–35 (2011)
12. High-Level Expert Group on Artificial Intelligence, European Commission, Ethics Guidelines for Trustworthy AI (2019); OECD, OECD Principles on Artificial Intelligence (2019); UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
13. Ian J. Goodfellow et al., Generative Adversarial Nets, in Advances in Neural Information Processing Systems 2672 (2014).

14. INDIA CONST. art. 14.
15. INDIA CONST. art. 19(1)(a).
16. INDIA CONST. art. 19(2).
17. INDIA CONST. art. 21.
18. INDIA CONST. arts. 14, 19 & 21; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
19. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021).
20. Information Technology Act, No. 21 of 2000, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).
21. Information Technology Act, No. 21 of 2000, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023); Copyright Act, No. 14 of 1957, India Code (1957)
22. Information Technology Act, No. 21 of 2000, INDIA CODE (2000); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021); Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).
23. Information Technology Act, No. 21 of 2000, S. 66D, India Code (2000).
24. Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183 (2016).
25. Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (2019).
26. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
27. K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India); Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India); Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1 (India).
28. Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Reg. & Governance 505 (2018).

29. Luciano Floridi, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities, 21 Minds & Mach. 689 (2019).
30. Ministry of Electronics & Information Technology, Digital India Programme, Government of India (2025).
31. Ministry of Electronics & Information Technology, Government of India, Advisory to Intermediaries and AI Platforms on Due Diligence Obligations Under the IT Rules, 2021 (Mar. 1, 2024).
32. Ministry of Electronics & Information Technology, Report of the Advisory Group on AI Governance (2024); NITI Aayog, Responsible AI for All: Operationalizing Principles for Responsible AI (2021).
33. Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 S.C.C. 353; Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1.
34. Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).
35. Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019).
36. Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399 (2017).
37. See, e.g., Cal. Elec. Code §§ 20010–20012 (regulating deceptive election-related deepfakes); Tex. Elec. Code Ann. S 255.004.
38. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.
39. Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach 1–30 (4th ed. 2021).
40. Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach 22–39 (4th ed. 2021).
41. Subramanian Swamy v. Union of India, (2016) 7 S.C.C. 221.
42. UNESCO, Guidance for Generative AI in Education and Research 8–20 (2023).
43. UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

 (ISSN: 2583-7753)