

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

A Comparative Analysis of Artificial Intelligence Regulatory Frameworks in India and European Union

DR. NIMISHA MISHRA* AND DR. T.V. RAJESH**

ABSTRACT

In terms of day-to-day work, artificial intelligence has not only been an invaluable resource to working professionals, as it has become essential to be able to use such technology to deal with the constantly changing cyber world. However, an unmanaged or inadequately monitored technology-driven workspace can pose a significant risk to stakeholders. There is a significant risk of bias because AI can think as closely as a human. Instances where AI has impersonated a human during a call and obtained funds sent to an account without authorization demonstrate that AI has presented significant risks. One such case occurred at a British energy company in March 2019, in which a telephone call appeared to come from the chief executive of the parent company demanding the immediate transfer of approximately EUR 220,000. There are also cases of photographs of people altered by AI being shared on social media; in December 2025 the Bombay High Court ordered the removal of AI-generated images of the actor Shilpa Shetty. The swift growth of digital marketplaces and data-driven government has elevated the security of personal data to a fundamental constitutional, economic, and human rights issue. The first comprehensive, legally enforceable and AI-specific legislation in the world, the European Union Artificial Intelligence Act (2024), controls AI using a systematic, risk-based approach. It divides AI systems into unacceptable risk, high risk, limited risk and minimal risk categories. It also places stringent compliance requirements on high-risk systems, especially those employed in the healthcare, education, employment and law enforcement sectors. While simultaneously regulating sophisticated general-purpose AI models, the Act places a strong emphasis on responsibility, transparency, human oversight and the defence of fundamental rights. India's Digital Personal Data Protection Act, 2023 is the country's first complete regulatory framework managing digital personal data, adopting a digital-first, risk-based strategy adapted to India's governance circumstances. India nevertheless lacks a dedicated AI-specific statute. Although the Digital Personal Data Protection Act, 2023 addresses data privacy concerns, it does not comprehensively regulate AI systems, risk classification, algorithmic accountability, or systemic harms such as deep fakes and automated decision-

* Author is the Principal at Pt. Kishorilal Shukla Vidhi Mahavidyalaya, Rajnandgaon, Chhattisgarh, India.

** Author is an Academic Advisor at Bhuvana Jyothi Institute of Legal Studies, Shirthyady, Dakshina Kannada, Karnataka, India.

making biases. Consequently, India's AI governance remains fragmented and largely policy-driven, revealing a significant regulatory gap when compared to the structured and rights-based framework adopted by the European Union. This study assesses whether India needs a specific AI law by comparing the advantages of the EU's comprehensive legislative approach with India's current legal framework. It concludes by offering suggestions for creating a fair, innovative and rights-protective AI regulatory framework that is in line with India's constitutional ideals, socioeconomic conditions and technical goals.

Keywords: Artificial Intelligence, GDPR, EU AI Act, Digital Personal Data Protection Act 2023, AI Governance

I. INTRODUCTION

The emergence of Artificial Intelligence (AI) has brought about significant transformations in modern society, particularly by influencing the manner in which decisions are made across various sectors. In the private sector, AI technologies are extensively employed for activities such as customer profiling, targeted advertising, and moderation of online content. Similarly, public authorities have also begun integrating AI into governance mechanisms, including public administration, predictive policing, and the implementation of welfare programmes. Despite these advantages, the increasing deployment of AI has raised serious concerns relating to individual privacy, procedural fairness, and accountability. These issues are further intensified by the rapid expansion of digital technologies and the large-scale generation and collection of data within the country.

Since the Hon'ble Supreme Court of India has recognised the right to privacy as a fundamental right¹, the growing use of AI across different sectors raises important constitutional considerations. However, India currently does not possess a specific and comprehensive legislative framework dedicated exclusively to the regulation of artificial intelligence. At present, issues associated with AI are largely addressed through existing statutory mechanisms, primarily the provisions of the Information Technology Act, 2000² and the rules framed thereunder. More recently, certain provisions of the Digital Personal Data Protection Act, 2023³ have also become relevant in the context of data processing involving AI technologies. Additionally, the provisions of the Bharatiya Nyaya Sanhita, 2023 may also apply in appropriate situations. In contrast, the European Union has taken a proactive legislative approach by

¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

² Information Technology Act, No. 21 of 2000, §§ 43A, 66, 72A, India Code (2000).

³ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

introducing the Artificial Intelligence Act, 2024⁴. The primary objective of this legislation is to promote transparency, safeguard fundamental rights, and regulate AI systems through a structured risk-based framework. Under this approach, AI systems are categorised into four distinct risk levels, namely (i) unacceptable risk, (ii) high risk, (iii) limited risk, and (iv) minimal risk⁵.

This research paper seeks to examine whether India requires a dedicated statutory framework to effectively address the legal and regulatory challenges arising from the use of artificial intelligence. By analysing the provisions of the EU Artificial Intelligence Act and comparing them with the existing regulatory structure in India, the study aims to contribute to the developing legal discourse on the governance of emerging technologies.

II. UNDERSTANDING ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is a technology that makes it possible for computers and other machines to carry out tasks like language comprehension, image recognition, decision making and problem solving that often require human intelligence. AI operates by utilizing videos and historical behaviour. These systems employ learning techniques to assist the machine in identifying links and patterns in the data. For instance, while some AI systems learn by trial and error (e.g. figuring out the optimal path in navigation apps) others learn by being taught with examples (e.g. recognizing a face in hundreds of photographs). AI frequently makes use of systems like computer vision (understanding photos and videos) Machine learning (learning from data) Neural networks (systems molded after the human brain) and natural language processing (understanding human language). AI follows pre programmed rules and learning patterns to produce outcomes even if it may seem intelligent. It does not think or feel like humans.⁶

III. USE, MISUSE AND ABUSE OF ARTIFICIAL INTELLIGENCE AND THE NEED FOR REGULATION

Aspect	Meaning	Examples	Problems Created	Why Regulation Is Needed
Use of AI	Appropriate, moral and advantageous use of AI for general	Medical service; Traffic management;	Generally advantageous; Increases accuracy	To guarantee ethical standards dependability and

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).

⁵ Regulation (EU) 2024/1689, arts. 5–9 (Artificial Intelligence Act) (classifying AI systems into unacceptable risk, high risk, limited risk and minimal risk).

⁶ Jennifer Monahan, Artificial Intelligence, Explained (Heinz College, Carnegie Mellon University July 2023), <https://www.heinz.cmu.edu/media/2023/July/artificial-intelligence-explained>

Aspect	Meaning	Examples	Problems Created	Why Regulation Is Needed
	welfare.	Aiding farmers to get an idea of weather forecast; Chat bots for customer service	and efficiency	safety.; To stop future abuse
Misuse of AI	Inappropriate negligent or reckless application of AI	AI hiring tools that may be biased; People being mistakenly identified by facial recognition; AI providing incorrect or medical advice	Disparities; Making poor choices; A decline in faith in technology	To establish rules for accountability; To require human oversight and audits
Abuse of AI	AI used maliciously and on purpose to hurt people or society	Widespread citizen monitoring; Blackmail using deepfakes; Fake news produced by AI; Cybercrime driven by AI	Invasion of privacy; A danger to democracy; Manipulation and social fear	To defend fundamental rights; To stop power abuse
; Sovereignty and National Security Issues in the Digital & AI Era;	; Sovereignty and National Security Issues in the Digital & AI Era;	; Sovereignty and National Security Issues in the Digital & AI Era;	; Sovereignty and National Security Issues in the Digital & AI Era;	; Sovereignty and National Security Issues in the Digital & AI Era;

Table 1: Use, misuse and abuse of artificial intelligence, and the regulatory need arising from each.

IV. THE EU ARTIFICIAL INTELLIGENCE ACT

The European Union recognized that while artificial intelligence has the potential to produce major social and economic benefits, if it is not appropriately regulated, it poses serious hazards to democratic processes, basic rights and rule of law. It was shown that earlier legal frameworks such as the General Data Protection Regulation (GDPR) were insufficient to handle issues unique to AI such as algorithmic bias, opaque automated decision-making, the usage of autonomous systems and widespread surveillance activities.

The European Union introduced the EU Artificial Intelligence Act to close this regulatory gap, creating the world's first comprehensive and legally enforceable framework dedicated solely to AI regulation. The Act's main goal is to guarantee that AI systems used in the EU are transparent, safe, dependable and focussed on human values.⁷

A. Risk Framework Summary

Category	Examples	Main Legal Effects
Banned Practices	Real time biometric identification	Total prohibition not allowed on

⁷ Reg. 2024/1689, art. 1 (subject matter and objectives: promoting human-centric and trustworthy artificial intelligence while ensuring a high level of protection of health, safety and fundamental rights).

Category	Examples	Main Legal Effects
	in public; Secret behaviour manipulation; Social grading by public authority	EU market.
AI and high risk	AI for safety critical infrastructure credit worthiness evaluation and hiring tools that influence hiring decisions	Subject to stringent compliance requirements and conformance evaluation.
Transparency requirements	Self-identifying chat bots and artificial media that need to be labelled.	User information and disclosure.
Minimal risk	Features that allow for consumer customisation.	Beyond general law there are no other legal requirements.

Table 2: Risk categories under the EU Artificial Intelligence Act and their principal legal effects. Source: Regulation (EU) 2024/1689, arts. 5, 6-9, 52-54 and 69.

V. AI-SPECIFIC LEGISLATION: THE CURRENT POSITION IN INDIA

Unlike the European Union, India does not currently have a formal legislative framework governing artificial intelligence. As a result, India now lacks a number of crucial regulatory protections found in the framework of the European Union.

A. What India Is Missing, Compared to the EU AI Act

Area	EU AI Act Provides	India Currently Lacks
AI- Specific legislation	Regulation of dedicated binding	Only policies and advisories
Classification based on risk	Unambiguous AI risk categories	No legal risk classification
Prohibition on harmful AI	Indeed e.g. Social scoring	No clear prohibition
Rules for AI accountability	Unambiguous accountability	Legal ambiguity
Bias control	Mandatory bias testing	No mandatory audits
Human oversight	Legally required	Not compulsory
AI transparency	Mandatory disclosures	Voluntary only
AI regulator	Designated authorities	No dedicated AI regulator

Table 3: Provisions of the EU Artificial Intelligence Act with no counterpart in Indian law.

B. Recent AI-Related Regulatory Developments in India

Although India does not yet have a dedicated Artificial Intelligence statute, certain regulatory developments have emerged in recent years. One important development is the amendment of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, including amendments introduced in 2026, which address issues relating to AI-generated content and algorithmic manipulation.⁸

⁸ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

The amended rules introduce the concept of “synthetically generated information,” referring to digital content such as audio, video, or images that are artificially created using computer technologies but appear authentic to viewers.⁹

Examples include deepfake videos, AI-generated voice cloning, synthetic political propaganda and manipulated visual content.

The rules impose several due diligence obligations upon digital intermediaries, including social media platforms and platforms that enable AI-based content creation.

i. Key Safeguards Introduced

AI generated content must be labelled: In order for users to recognize that the content is artificially created, platforms must make sure that synthetic media is properly marked.

Technical defences against illicit AI content: To stop the creation of illegal synthetic content such as deep fake pornography or deceptive digital impersonation , intermediaries must implement automated techniques.

Traceability via IDs and metadata: Technical identifiers or metadata that allow authorities to track down the source of synthetic content must be included.

Quick elimination of illegal AI content: After being informed , the platforms are required to remove unlawful content within predetermined time frames.

A process for resolving user grievances: Grievances officers must be appointed by platforms and complaints must be resolved within the allotted time frames.

These provisions indirectly contribute to regulating AI-generated content by promoting transparency, traceability, and accountability within digital platforms.

VI. EMERGING AI LEGISLATIVE FRAMEWORK IN INDIA

In addition to the rules introduced under the IT Act to regulate the technology, the Government of India has issued certain guidelines for governance of AI and the MANAV framework, focusing on responsible and ethical AI development.¹⁰ These guidelines and MANAV, which represents Moral and Ethical Systems, Accountable Governance, National Sovereignty, Accessibility and Inclusivity, Validity and Legitimacy, emphasise on development of safe, trustworthy, socially inclusive and beneficial AI. The MANAV framework, which was proposed by the Hon’ble Prime Minister of India at the AI Impact Summit, 2026 at New Delhi envisages

⁹ Id.

¹⁰ Ministry of Electronics and Information Technology, Government of India, *India AI Governance Guidelines*, issued under the IndiaAI Mission, 5 November 2025.

a human-centric approach to AI governance. These guidelines, albeit without the legal support for enforcement, portray the attempts of the country for designing regulatory structure for AI in India.

Despite the fact that India has been addressing the challenges posed by the AI to a great extent by appropriately introducing rules under the IT Act, by timely amending the said rules, and by introducing policy frame work, the country is yet to have a comprehensive law with regard to AI technology. However, the good news is that the country has been working in this direction, in order to introduce a formal and structured legal frame work and discussions are being held in this regard on the Artificial Intelligence (Ethics and Accountability) Bill, 2025, which has been introduced in the Lok Sabha as a private member's bill.¹¹

The draft Bill covers various aspects of regulation such as (i) establishment of an AI Ethics Committee, (ii) mandatory ethical assessment of high-risk AI systems (iii) grievance redressal procedures for affected individuals (iv) fairness audits to mitigate algorithmic bias (v) ensuring transparency (vi) deterrence by way of imposing penalties etc. The introduction of such a private bill with contents as discussed reflects the level of awareness in India with regard to the requirement of statutorily regulating the artificial intelligence technologies.

VII. JUDICIAL RECOGNITION OF PRIVACY AND DATA PROTECTION IN INDIA

The enormous ability of AI to intrude into the privacy of citizens can never be overstated. Despite the absence of a legislation in this regard, the Hon'ble Supreme Court of India has recognised the importance of the fundamental right of privacy and informational autonomy in the digital era. In the case of Justice Puttaswamy, the Hon'ble Apex Court established a constitutional basis for data protection and digital rights, by holding that privacy of a citizen is an integral part of fundamental rights guaranteed under Article 21 of the Constitution of India.¹²

In the case of Anuradha Bhasin, the Hon'ble Court underscored the necessity to protect civil liberties in the digital environment by holding that any restriction on internet access or digital communication must satisfy the principles of necessity and proportionality, thereby emphasising the need to protect civil liberties in the digital environment.¹³

In *Internet and Mobile Association of India v. Reserve Bank of India*, the Hon'ble Supreme Court of India struck down a circular dated 6th April, 2018 issued by the RBI on the ground that the restrictions imposed vide the said circular, being subordinate legislation, were

¹¹ The Artificial Intelligence (Ethics and Accountability) Bill, 2025, Bill No. 59 of 2025 (India), introduced in the Lok Sabha on 17 December 2025 as a private member's bill.

¹² *Puttaswamy*, supra note 1.

¹³ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

disproportionate to the concerns raised by RBI. It was held that such a measure by the RBI would wipe out Virtual Currency exchanges ‘out of the industrial map of the country, thereby infringing Article 19(1)(g)’ and therefore it is necessary to pass the test of proportionality. Thus, the Apex court reiterated that regulation in emerging technological sectors must maintain a balance between encouraging innovation and protecting constitutional rights.¹⁴

The decisions of the highest judiciary as above, will have an influence on the governance of emerging technologies, including AI, in ensuring constitutional protections relating to privacy, dignity, and freedom.

VIII. ANALYTICAL OBSERVATION

The comparative analysis indicates that the GDPR of the EU and the DPDP Act of India, which are basically designed for data protection, are not able to effectively regulate the AI technology, especially with regard to ethical issues, bias that can be caused due to the algorithmic designs. They can be used for regulating only a portion of the use of the AI technology. The EU AI Act was born out of the inadequacy of the GDPR with regard to AI, thereby creating an exclusive framework for AI governance. On the other hand, India’s regulation of AI is multi-faceted, including the guidelines on ethics, which are largely unenforceable, due to the absence of specific statute.

A. Areas Where India Needs to Learn from the EU

EU AI Act being the first in the world in order to exclusively regulate the AI technology, India may adopt the best practices and regulatory model, that may be suitable to the country and in line with the provisions of the constitution.

i. Enacting a Dedicated AI Law

A comprehensive and exclusive AI law at the federal level, ensuring uniform regulatory standards across the country will go a long way in ensuring compliance by the platforms as well as ethical usage by the customers.

ii. Establishing Risk-Based Classification

Since the applicability of AI and the risk involved therein are different, based on various circumstances, classifying the regulatory scrutiny into different levels, as in the case of EU AI Act, would be beneficial as well as easy to implement.

¹⁴ Internet & Mobile Ass’n of India v. Reserve Bank of India, (2020) 10 SCC 274.

iii. Mandatory Algorithmic Audits

While the systems collect huge data that are mainly sensitive in nature, regular evaluation of at least important sectors such as employment, finance, healthcare etc. may be considered to be brought under Mandatory Algorithmic Audit, in order to ensure that there is no bias based on the analysis of the data.

iv. Stronger Transparency Requirements

Individuals should be clearly informed when they are interacting with the AI systems, so that it reduces the risk of deception, promotes trust, and enables informed decision making. Providing information about the use, scope and limitations to the user ensures enhanced accountability on the part of the service provider.

v. Regulation of AI Surveillance

The AI systems which utilise the bio-metric data and are employed in surveillance systems have the ability to store the data and intrude into the privacy of a user. Therefore, appropriate legal safeguards need to be incorporated in such systems, in the interest of the individuals.

IX. POLICY RECOMMENDATIONS FOR REFORM

A. Expand Scope to Include Offline Personal Data

Under the DPDP Act, the personal data collected offline are beyond the purview of the legal framework. However, when integrated with AI, the offline data can be utilised by the system for analysis in view of the targeted purpose. Therefore, bringing the offline personal data under the purview of the enacted law would be in the interest of the citizen.

B. Strengthen Individual Rights

Provisions need to be made in law for incorporating rights regarding deletion of data, portability of service providers, and for safeguards against algorithmic decision making, so as to enhance autonomy and choice of the individual.

C. Narrow and Procedural State Exemptions

Unlike in the case of DPDP Act, broad exemptions should not be granted to the Government when it comes to AI regulation, as that could lead to mass surveillance and intrusion to privacy and infringement of fundamental rights.

D. Creation of an Independent and Transparent Regulatory Authority

Since the regulation of AI technology is a complex matter, wherein the regulator needs to be updated about the latest in the technology, an independent authority may be considered for the

purpose. Further, posting the officials for a fixed tenure will provide them with functional independence, while improving the accountability.

X. CONCLUSION

The comparative analysis of artificial intelligence governance in the European Union and India primarily differ in the regulatory approaches. As on date, the EU has established a comprehensive legal framework, the AI Act, being the first statute in the world for regulating the technology of AI. By classifying the systems and imposing restrictions accordingly, the AI Act of EU has either prohibited or strictly controlled the technology, thereby positioning themselves as a global leader in governing and regulating AI technology in a responsible manner. While protecting the basic fundamental rights and ensuring accountability, the AI Act has also taken into account the scope of human oversight.

On the other hand, India is yet to enact an exclusive, codified law for regulating AI. However, provisions of the IT Act, which was primarily designed for according legal recognition for electronic transactions, are being used in India for this purpose, by introducing rules and appropriately amending them. Further, certain provisions of the DPD Act and the Bharatiya Nyaya Sanhita, exclusive guidelines issued in this regard, the MANAV framework are being utilised to regulate unscrupulous activities such as deepfake, misinformation, algorithmic bias etc. While these fragmented regulations support innovation and development of technology, it gives scope for gaps in certain areas such as classification of risk, oversight of biometric surveillance, algorithmic accountability etc.

Thus, the comparison indicates that the approach of the EU is preventive regulation, while protecting the rights of individuals, whereas the focus of India is more on promoting innovation and gradual development of regulatory framework.

Nevertheless, with the latest policy initiatives, regulatory reforms and proposed legislation, India is moving forward towards a structured governance model. With the EU model already available to analyse the pros and cons, India can develop a regulatory framework, simultaneously protecting the fundamental rights and encouraging innovations and technological advancements.

Thus to conclude, the ability of the country to transform the fragmented regulatory structure into a comprehensive legal framework will decide the future trajectory of artificial intelligence governance in India. Achieving the balance of protection of fundamental rights and the innovation driven development will be crucial to ensure that the AI technology functions as a tool for social progress, economic development, and democratic accountability.