
REGULATING ARTIFICIAL INTELLIGENCE IN INDIA: LEGAL AND CORPORATE CHALLENGES

Adv. Tushar Gajanan Raut

ABSTRACT

The increasing integration of Artificial Intelligence (AI) into India's economic and governance structures has generated significant legal and corporate concerns that existing regulatory mechanisms are not fully equipped to address. AI-driven systems are now widely used in sectors such as finance, healthcare, and e-commerce, where automated decision-making plays a crucial role. In this context, the present paper seeks to examine the adequacy of India's current legal framework in regulating AI technologies, particularly in relation to issues of liability, accountability, transparency, and corporate responsibility. It further explores whether India is institutionally and legally prepared to respond to the risks posed by autonomous and data-driven systems. This study adopts a doctrinal research methodology, based on the analysis of statutory provisions, policy initiatives, and comparative legal frameworks. It evaluates the applicability of existing laws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, while also drawing comparisons with international standards like the General Data Protection Regulation and the proposed EU AI Act. This comparative approach helps in identifying gaps and best practices relevant to AI governance. The findings of the study indicate that the current Indian legal framework is fragmented and lacks specific provisions to address AI-related risks such as algorithmic bias, opacity in decision-making, and unclear allocation of liability. It is observed that corporations deploying AI technologies often function without clearly defined accountability structures, thereby raising legal and ethical concerns. The paper concludes that there is an urgent need for a comprehensive and principle-based regulatory framework that ensures transparency, fairness, and accountability, while also promoting innovation. Strengthening corporate compliance mechanisms and adopting a risk-based regulatory approach are essential for effective AI governance in India.

Key Words: - Artificial Intelligence, Corporate Liability, Data Protection, Algorithmic Bias, AI Regulation, Corporate Governance, Compliance, Risk-Based Regulation, Cyber Law, Digital Personal Data Protection Act

I. Introduction

Artificial Intelligence (AI) has emerged as a transformative force reshaping modern economies, governance structures, and societal interactions. In India, the adoption of AI technologies has accelerated across sectors such as finance, healthcare, e-commerce, and public administration¹. From automated credit scoring systems and algorithmic trading to facial recognition and predictive policing, AI is increasingly influencing decision-making processes that were traditionally dependent on human judgment. While these developments promise enhanced efficiency, accuracy, and innovation, they simultaneously raise complex legal and regulatory concerns that challenge existing frameworks.²

One of the primary issues associated with AI systems is the lack of transparency in their functioning. Many advanced AI models operate as “black boxes,” where the logic behind decisions is not easily interpretable.³ This creates significant challenges in determining accountability, particularly in situations where AI systems produce erroneous or discriminatory outcomes. The problem is further compounded by the phenomenon of algorithmic bias, where AI systems may replicate or even amplify existing social inequalities embedded within training data. Such outcomes raise serious concerns in light of constitutional principles of equality and fairness.

In addition to concerns of transparency and bias, the extensive reliance of AI systems on large volumes of personal data has intensified issues relating to privacy and data protection. The recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* has added a constitutional dimension to data governance in India, thereby necessitating stricter scrutiny of data-driven technologies. Despite legislative developments such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, the Indian legal framework remains fragmented and insufficient to address the unique challenges posed by AI.

From a corporate perspective, the integration of AI introduces new dimensions of risk and responsibility. Companies deploying AI systems are required to ensure compliance not only with

¹ NITI Aayog, National Strategy for Artificial Intelligence #AIforAll 1–10 (2018)

² Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147, 1150–55 (2017)

³ Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 3–15 (2015)

existing legal standards but also with emerging expectations relating to ethical AI practices and accountability. However, the absence of clear regulatory guidelines often results in uncertainty regarding liability and governance obligations. This is particularly problematic in cases where AI systems operate autonomously, making it difficult to attribute responsibility for harmful outcomes.

Against this backdrop, the need for a comprehensive and forward-looking regulatory framework for AI in India becomes increasingly evident. Such a framework must strike a balance between fostering innovation and safeguarding fundamental rights, while also ensuring that corporations remain accountable for the technologies they deploy. This paper seeks to critically examine the legal and corporate challenges associated with AI regulation in India and to propose a structured approach for effective governance in the evolving technological landscape.

II. Research Methodology

This study adopts a doctrinal method of legal research, focusing on the analysis and interpretation of existing legal frameworks governing Artificial Intelligence (AI) in India.⁴ The approach primarily examines statutory provisions such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, along with relevant judicial decisions. Landmark cases like *Justice K.S. Puttaswamy v. Union of India* and *Shreya Singhal v. Union of India* have been considered to understand the evolving constitutional principles relating to privacy, freedom of speech, and digital governance.⁵

This study uses both primary and secondary resources. The primary sources of information include case law, legislation, and regulatory rules; while the secondary sources are scholarly articles, policy reports, and commentary on the law. These resources have all been reviewed critically in order to determine whether or not the current legal framework adequately addresses AI-related issues such as liability, algorithmic bias and corporate accountability.

A comparison of the global regulations surrounding this topic, including the General Data Protection Regulation (GDPR) and the proposed EU AI ACT, is included to gain further clarity about potential gaps in the regulation of Artificial Intelligence (AI) in India. This will also allow

⁴ William Twining, *General Jurisprudence: Understanding Law from a Global Perspective* 203–05 (2009)

⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1; *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1

for lessons learned from other countries with respect to AI regulations to help develop an effective regulatory framework within India.

III. Conceptual Framework: AI and Legal Concerns

Artificial Intelligence (AI) represents a significant shift from traditional technological systems, as it enables machines to learn, adapt, and make decisions with minimal human intervention. This evolving nature of AI raises complex legal concerns that existing frameworks are not fully equipped to address. The key conceptual issues are outlined below:

A. Nature and Functioning of AI Systems

True software is made up of pre-defined rules whereas Artificial Intelligence systems operate by using algorithms, processing data and recognising patterns to replicate how humans think and behave using these technologies to process vast amounts of new incoming data to continue learning (through the more advanced forms) via machine learning and deep learning models that constantly evolve based upon their experiences with newly introduced information.⁶ As a result, AI is unique because of the unpredictable and constantly changing nature of these systems. Because of this dynamic characteristic of AI, regulatory frameworks must now address regulatory complexity that arises due to these systems being adaptive rather than fixed as they were originally intended to do so; therefore, they also pose challenges to applying the traditional principles of law that were designed to cover fixed, predictable and easily attributable actions committed by a defined person (or organisation).⁷

B. Opacity and Lack of Explain ability (Black Box Problem)

One of the most significant challenges in the regulation of artificial intelligence has come from the "black box" problem, in which the internal decision-making processes of artificial intelligence remain opaque. The lack of explain ability has caused significant challenges in establishing legal responsibility, accountability, and clear explanations for decisions⁸. It has challenged some of the most fundamental principles of natural justice.⁹ The "black box" problem

⁶ Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 28–35 (4th ed. 2020)

⁷ Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399, 404–10 (2017)

⁸ Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 Geo. L.J. 1147, 1160–65 (2017)

⁹ *Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248

has also raised significant challenges in the context of the "right to explanation," which has recently gained significant traction in international legal frameworks.

C. Algorithmic Bias and Discrimination

One of the major concerns regarding artificial intelligence is its potential to perpetuate biases and discriminate against different groups of people in important spheres of life such as employment, credit systems, and law enforcement. In the context of India, such biases in artificial intelligence have profound constitutional implications and may violate the constitutional principle of equality and non-discrimination provided by Article 14 of the Constitution of India, which provides for the equality of all citizens and requires that all citizens be treated without any form of arbitrary discrimination. However, addressing such biases is very difficult due to the opaque nature of artificial intelligence systems and the complex roles played by different stakeholders involved in the development of such systems, ranging from data collectors and trainers to deplorers.¹⁰

D. Autonomous Decision-Making and Liability Issues

As such, the operation of these systems with little or no human intervention is a significant disruption of traditional liability principles that have long been based on the concepts of intent, negligence, and human conduct. This is because of the uncertainty surrounding liability that arises when it is not clear if the liability lies with the developer, the deployed, the user, or even the AI system itself that is not yet recognized in law as a legal entity that is capable of being held accountable. The lack of clear fault lines in autonomous decision-making also poses a problem for traditional legal principles based on human foresight and control because such scenarios are not based on direct intent or even foreseeability by any of the players involved.¹¹

E. Data Privacy and Protection Concerns

The operational dependence of AI systems on large amounts of personal and sensitive information also heightens some of the more alarming issues, such as unauthorized processing, ubiquitous surveillance, and susceptibility to data breaches, which assume a higher constitutional

¹⁰ Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev. 671, 677–90 (2016)

¹¹ Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399, 401–10 (2017)

priority in India in light of the establishment of a fundamental right to privacy in the landmark case of Justice K.S. Puttaswamy v. Union of India.¹²

While legal frameworks such as the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 form a basic framework for data protection, they remain inadequate to address issues of artificial intelligence since they fail to include provisions on AI. Therefore, issues such as profiling, surveillance, and systemic risks associated with autonomous systems remain in a gray area, thereby raising a number of issues concerning individual rights protection against the unique risks of AI technologies.¹³

F. Corporate Accountability and Ethical Governance

As the role of artificial intelligence is being increasingly relied upon to aid decision-making processes and improve the efficiency of operations, the corporations involved in the process also assume the responsibility of using the technology ethically, transparently, and with proper risk management processes, which still remains undefined in the context of the country. As the lack of clear guidelines has led to the adoption of different approaches by corporations, which is risky and uncharted territory for them to operate in without any unified set of guidelines to govern the process, the newly developed term of algorithmic accountability is being increasingly used to ensure the importance of using the technology ethically, transparently, and with proper risk management processes, which is less about compliance with the lack of regulations and more about the organization's integrity and the integrity of the individuals affected.¹⁴

G. Tension between Innovation and Regulation

The call for the regulation of the development of artificial intelligence requires that the approach taken is flexible and innovative, but the challenge lies in finding the right balance between the two, as over-regulation can lead to the stifling of growth, while on the other hand, the lack of regulation can lead to legal uncertainty, with basic human rights vulnerable to violation. Therefore, the right approach is one that is balanced, flexible, and innovative, where the focus is on the laying down of basic principles rather than the imposition of strict regulatory guidelines that can easily be rendered obsolete with the rapid advancement of the technologies involved.

¹² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1

¹³ Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023)

¹⁴ Nicholas Diakopoulos, Accountability in Algorithmic Decision Making, 59 Commc'ns ACM 56, 56–62 (2016)

This will ensure that the regulation is not only innovative but also accountable, as well as in the best interest of the public, while at the same time ensuring that the advancement of the technologies is not stifled while the basic human rights of the people are protected.¹⁵

IV. Indian Legal Framework: Statutory and Judicial Analysis

1. Absence of a Dedicated AI Legal Framework

- The country lacks a specific legal framework which was designed to govern Artificial Intelligence (AI).
- The legal framework on AI in this particular country has been developed through a combination of various legal provisions and interpretations, which were originally designed to address other issues of information technology, etc.¹⁶

2. The Information Technology Act, 2000

- Regarded as the main legislation regarding cyber law in India.
- Accords legal validity to electronic records and outlines a framework for tackling cybercrimes and data protection.
- Section 43A makes corporate entities liable in cases of failure to adopt reasonable security practices in protecting sensitive information related to individuals.
- **Limitations:** The legislation has failed to address issues related to AI in general; therefore, it is not entirely effective in regulating AI systems.¹⁷

3. The Digital Personal Data Protection Act, 2023

- Represents a contemporary and organized effort to regulate data processing activities in India.
- Introduces the concept of data fiduciaries, which have responsibilities in connection with lawful processing, consent, and data security.
- Indirect Impact on AI: Since AI heavily depends on data, this legislation has an impact on AI governance through the control of personal data collection and processing.
- **Limitations:** The Act does not address other pertinent issues concerning AI, which makes its efficacy questionable in the context of AI governance.¹⁸

¹⁵ OECD, Recommendation of the Council on Artificial Intelligence 3–6 (2019)

¹⁶Karnika Seth, Artificial Intelligence: Law & Policy 215–20 (2021)

¹⁷Karnika Seth, Artificial Intelligence: Law & Policy 222–25 (2021)

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

- Imposes duties on intermediaries to exercise due diligence, which includes content moderation and grievance redressal.
- **Relevance:** Applicable to digital platforms using AI tools to filter and moderate content.
- **Limitations:** Does not offer a detailed guideline to govern the entire spectrum of AI technologies.¹⁹

5. Policy Initiatives and Non-Binding Frameworks

- NITI Aayog's strategy on Artificial Intelligence and guidelines on Responsible AI indicate the intent of promoting ethical practices in Artificial Intelligence.
- **Limitations:** These are in the nature of non-binding guidelines, which are not enforceable in any manner.²⁰

6. Judicial Pronouncements Shaping AI-Relevant Jurisprudence

a. Justice K.S. Puttaswamy v. Union of India (Privacy Judgment)

- Recognized the right to privacy as a fundamental right under Article 21 of the Constitution.
- Emphasized principles of legality, necessity, and proportionality to prevent arbitrary use of technology.
- The decision has far-reaching implications for AI governance, particularly with regard to data collection, surveillance, and profiling.²¹

b. Shreya Singhal v. Union of India (Freedom of Speech)

- Struck down Section 66A of the IT Act on the grounds that the right to freedom of speech and expression is violated.
- Stresses the need to ensure that regulatory measures in the cyber world, including those related to AI, do not restrict constitutional freedoms disproportionately.²²

¹⁸ Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–12, The Gazette of India (2023)

¹⁹ Karnika Seth, Artificial Intelligence: Law & Policy 260–63 (2021)

²⁰ NITI Aayog, Responsible AI for All: Guiding Principles 12–18 (Feb. 2021)

²¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, AIR 2017 SC 4161 (India)

²² Shreya Singhal v. Union of India, (2015) 5 SCC 1, AIR 2015 SC 1523 (India)

c. K.S. Puttaswamy (Aadhaar) v. Union of India (Data Proportionality)

- Upheld the Aadhaar scheme but with certain restrictions to ensure that the proportionality and security of the data collection process are maintained.
- The above judgment highlights the need to ensure the advancement of technologies while protecting the rights of individuals, which is equally relevant in the context of AI systems.²³

7. Inadequacy of the Current Legal Framework

This, however, has not translated into an efficient and proper regulation of artificial intelligence, considering that the existing legislative and judicial framework in the country remains inadequate in addressing the unique issues of artificial intelligence. This can be attributed to the fact that there remains a critical lack in the existing regulatory environment, which includes the lack of specific legislation to govern artificial intelligence, the lack of specific standards to govern algorithmic accountability, and the lack of specific mandates to ensure transparency and explain ability in artificial intelligence.²⁴

This means that the existing legislative and judicial framework in the country, which remains highly specific to data protection and intermediary liability, remains inadequate in governing the unique issues of artificial intelligence, which include the development of autonomous and intelligent systems that can perform functions with minimal human intervention. Therefore, the legislative and judicial framework in the country to govern artificial intelligence can only be regarded as fragmented and reactive, considering that it only attempts to govern artificial intelligence issues in an ad hoc manner.

V. Corporate Challenges in AI Regulation**A. Attribution of Liability**

One of the most pressing issues in the governance of AI is determining who is liable in case of a negative outcome of the system. The current legal system is not geared to deal with autonomous decision-making.

²³ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1, AIR 2019 SC 216 (India)

²⁴Karnika Seth, Artificial Intelligence: Law & Policy 300–10 (2021)

For instance, in a healthcare system where an AI system has made a wrong diagnosis, it becomes difficult to determine who is liable, the developer, the organization, or the system itself.

B. Corporate Governance and Risk Management

Corporations must also ensure that they incorporate strong governance structures to accommodate AI integration. This includes ensuring that boards of directors address technological risks, as well as legal and ethical compliance.

The term "algorithmic accountability" is gaining traction, and corporations must ensure that AI systems are transparent, fair, and auditable.

C. Compliance Challenges

Corporations face increasing compliance burdens due to evolving data protection laws and regulatory expectations. The absence of clear AI-specific guidelines further complicates compliance efforts.

D. Ethical and Reputational Risks

Failure to address ethical concerns such as bias and discrimination can result in reputational damage and legal liability. Companies must therefore integrate ethical considerations into their AI strategies

VI. Comparative Analysis: Global Regulatory Approaches

A. General Data Protection Regulation (GDPR)

The GDPR provides a comprehensive framework for data protection in the European Union. It includes provisions on automated decision-making and grants individuals the right to meaningful information about the logic involved.

B. EU AI Act

The proposed EU AI Act adopts a risk-based approach, categorizing AI systems into unacceptable, high-risk, limited-risk, and minimal-risk categories.⁷ High-risk systems are subject to stringent compliance requirements, including human oversight and transparency.

C. Case Law: International Perspective

In *Google Spain SL v. AEPD*, the Court of Justice of the European Union recognized the “right to be forgotten,” reinforcing data protection principles in the digital age.²⁵

D. Lessons for India

- Adoption of a risk-based regulatory framework
- Emphasis on transparency and explainability
- Establishment of clear liability mechanisms
- Strengthening of data protection and privacy laws

VII. Need for a Dedicated AI Regulatory Framework in India

India’s current regulatory approach is fragmented and reactive. There is an urgent need for a comprehensive framework that addresses AI-specific challenges.

A. Principle-Based Regulation

A principle-based approach focusing on fairness, accountability, transparency, and privacy would provide flexibility while ensuring ethical AI deployment.

B. Risk-Based Classification

AI systems should be categorized based on their potential risks, with stricter regulations for high-risk applications such as healthcare and law enforcement.

C. Institutional Mechanisms

The establishment of a dedicated regulatory authority could enhance oversight and ensure compliance with AI governance standards.

VIII. Recommendations

1. Enact a Comprehensive AI Law

A dedicated legislation should be introduced to regulate AI technologies.

²⁵ *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317, [2014] QB 1022, [2014] 2 W.L.R. 1265 (May 13, 2014)

2. Amend Existing Laws

The IT Act and DPDP Act should be updated to include AI-specific provisions.

3. Corporate Governance Reforms

Companies should implement internal AI governance frameworks, including risk assessments and audits.

4. Judicial Oversight

Courts should continue to play an active role in safeguarding fundamental rights in the context of AI.

5. International Collaboration

India should align its regulatory framework with global standards.

IX. Conclusion

Artificial Intelligence represents both an opportunity and a challenge for India's legal and corporate landscape. While AI has the potential to drive innovation and economic growth, it also raises complex issues related to accountability, transparency, and data protection.

The existing legal framework in India is inadequate to address these challenges comprehensively. Judicial developments have provided some guidance, but a dedicated legislative framework is necessary to ensure effective regulation.

By adopting a balanced approach that integrates innovation with accountability, India can establish a robust AI governance framework that protects fundamental rights while promoting technological advancement.

References

1. Karnika Seth, *Artificial Intelligence: Law & Policy* (2021)
2. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015)
3. Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed. 2020)
4. William Twining, *General Jurisprudence: Understanding Law from a Global Perspective* (2009)
5. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671 (2016)
6. Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399 (2017)
7. Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 Geo. L.J. 1147 (2017)
8. Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making*, 59 Commc'ns ACM 56 (2016)
9. Digital Personal Data Protection Act, 2023, No. 22 of 2023, *reprinted in* The Gazette of India (2023)
10. Information Technology Act, 2000, No. 21 of 2000, *reprinted in* The Gazette of India (2000)
11. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), *reprinted in* The Gazette of India (Feb. 25, 2021)
12. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, AIR 2017 SC 4161 (India)
13. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1, AIR 2019 SC 216 (India) (*Aadhaar* judgment)
14. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248, AIR 1978 SC 597 (India)
15. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, AIR 2015 SC 1523 (India)
16. *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI: EU:C:2014:317, [2014] QB 1022, [2014] 2 W.L.R. 1265 (May 13, 2014)
17. NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (2018)
18. NITI Aayog, *Responsible AI for All: Guiding Principles* (Feb. 2021)

19. OECD, *Recommendation of the Council on Artificial Intelligence* (2019)