International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Inadequacy of the IT Act, 2000 in Governing Artificial Intelligence: Need for Legal Reform

Tushar Sahu[1]and Dr. Rajeev Singh[2]

[1]Student, LLM in Cyber Laws and Cyber Securities, Amity Law School, Amity University Lucknow Campus
[2]Assistant Professor, Amity Law School, Amity University Lucknow Campus

Abstract
The rapid growth of Artificial Intelligence (AI) has fundamentally reshaped the digital landscape, influencing how decisions are made, services are delivered, and data is processed across sectors. From automated financial systems to predictive policing and healthcare diagnostics, AI is no longer a futuristic concept but a present-day reality. However, this technological progress has also introduced complex legal, ethical, and regulatory concerns that existing laws struggle to address. In India, the primary legislation governing digital activities—the Information Technology Act, 2000—was enacted at a time when AI technologies were either non-existent or in their infancy. Consequently, the Act is not equipped to deal with the nuanced challenges posed by modern AI systems.
One of the major concerns is the lack of clear accountability when AI systems make decisions independently. Issues such as algorithmic bias, where AI systems may produce discriminatory outcomes, and the absence of transparency in automated decision-making raise serious questions about fairness and justice. Additionally, determining liability for harm caused by AI—whether it lies with developers, users, or organizations—remains unclear under the current legal framework.
This paper seeks to critically analyse these gaps within the IT Act and highlights the urgent need for reform. By examining international approaches to AI regulation, it aims to provide meaningful insights for India to develop a robust, future-ready legal framework that balances innovation with accountability and protection of individual rights.

Keywords: Artificial Intelligence, IT Act 2000, Legal Reform, Algorithmic Accountability, Cyber Law

Introductions

Artificial Intelligence (AI) has emerged as a transformative force across multiple sectors, fundamentally altering the way society's function and economies operate. In healthcare, AI is used for diagnostics and predictive treatment; in finance, it enables algorithmic trading and fraud detection; in agriculture, it supports precision farming; and in criminal justice, it assists in surveillance and risk assessment. These systems are capable of performing complex tasks such as decision-making, pattern recognition, and predictive analysis—functions that were traditionally dependent on human intelligence. The increasing

[1] Student, LLM in Cyber Laws and Cyber Securities, Amity Law School, Amity University Lucknow Campus
[2] Assistant Professor, Amity Law School, Amity University Lucknow Campus

reliance on AI has not only improved efficiency but also raised significant concerns regarding fairness, accountability, and ethical governance.[3]

Despite these advancements, the legal framework in India has not evolved at the same pace. The Information Technology Act, 2000, which serves as the cornerstone of India's cyber law regime, was enacted with the primary objective of facilitating electronic commerce and addressing cyber offences.[4] While the Act has undergone amendments, particularly in 2008, its provisions remain largely focused on conventional digital issues such as hacking, identity theft, and data breaches. It does not adequately contemplate the complexities introduced by AI technologies, such as autonomous decision-making, machine learning processes, and algorithmic opacity.

This mismatch between technological advancement and legal regulation has created a significant regulatory vacuum. Issues such as algorithmic bias, lack of transparency in AI systems, and ambiguity in assigning liability for AI-driven harm remain unaddressed. Furthermore, the deployment of AI in sensitive areas raises concerns about potential violations of fundamental rights, including the right to privacy and equality.[5] In the absence of a comprehensive legal framework, there is an urgent need to reassess and reform existing laws to ensure that technological innovation is balanced with accountability and the protection of individual rights.

Understanding Artificial Intelligence and Its Legal Implications

Artificial Intelligence (AI) refers to the capability of machines and computer systems to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, and decision-making. Unlike traditional software, AI systems are designed to adapt and improve over time through exposure to data. This dynamic nature is primarily driven by machine learning techniques, where algorithms identify patterns and make predictions without explicit programming. One of the defining features of AI is autonomy, which enables systems to operate with minimal or no human intervention. This is particularly evident in applications such as autonomous vehicles, automated financial systems, and predictive policing tools. Another key characteristic is self-learning capability, where AI models evolve by continuously processing new data inputs, often leading to outcomes that even developers may not fully anticipate. Additionally, AI systems rely heavily on data-driven decision-making, where large datasets are analysed to generate insights and predictions, making data the backbone of AI functionality.[6]These features, while beneficial, give rise to significant legal implications. The lack of human control in AI-driven decisions challenges traditional legal principles that assume human agency and intent. Furthermore, AI systems may perpetuate or even amplify bias and discrimination, especially when trained on flawed or unrepresentative datasets, leading to unfair outcomes in areas such as hiring, lending, and law enforcement.[7]Another critical concern is the potential for privacy violations, as AI systems process vast amounts of personal data, often without adequate safeguards or informed consent. Lastly, there is considerable ambiguity in determining liability when AI systems cause harm. It remains unclear whether responsibility should lie with the developer, the user, or the organization deploying the technology. This uncertainty highlights the

[3] *Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach (3rd ed., Pearson, 2010).*
[4] *Information Technology Act, 2000 (Act No. 21 of 2000).*
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*
[6] *NITI Aayog, National Strategy for Artificial Intelligence (2018).*
[7] *Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact," (2016) 104 California Law Review 671.*

inadequacy of existing legal frameworks and underscores the need for a more nuanced regulatory approach to AI governance.[8]

Overview of the Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) was enacted as India's primary legislation to regulate activities in the digital domain and to provide a legal framework for electronic governance and cybersecurity. The Act was introduced in response to the growing use of electronic communication and e-commerce, aiming to bring legal certainty to digital transactions. Its primary objectives include granting legal recognition to electronic records and digital signatures, thereby facilitating online contracts and business transactions.[9]Additionally, the Act seeks to prevent cybercrime by defining and penalising various forms of unauthorized access and misuse of computer systems. It also promotes e-governance by enabling the filing, storage, and processing of documents in electronic form by government agencies. The Act contains several important provisions to address cyber offences and data protection concerns. Section 43 imposes civil liability for unauthorized access, downloading, or extraction of data from computer systems, and provides compensation for damages caused. Section 66 criminalises computer-related offences such as hacking, identity theft, and dishonest or fraudulent access to digital systems. Section 72 deals with the breach of confidentiality and privacy, penalising individuals who disclose personal information obtained through lawful access without consent. These provisions collectively form the backbone of India's cybersecurity regime. Despite its significance, the IT Act reflects the technological realities of the early 2000s. Although the 2008 amendment introduced certain updates, including provisions related to data protection and cyber terrorism, the Act remains largely focused on traditional cyber issues such as hacking and electronic fraud. It does not adequately address emerging technologies like Artificial Intelligence, which involve autonomous decision-making, complex data processing, and algorithmic governance. This limitation highlights the growing gap between existing legal frameworks and modern technological developments, necessitating comprehensive reform to ensure effective regulation in the digital age.[10]

Inadequacies of the IT Act, 2000 in Governing AI

The Information Technology Act, 2000, though foundational to India's digital legal framework, is increasingly inadequate in addressing the complexities introduced by Artificial Intelligence. Its limitations become evident when examined in the context of modern AI systems, which operate in ways that were not envisioned at the time of the Act's enactment.

4.1 Absence of AI Definition and Scope

One of the most fundamental gaps in the IT Act is the absence of any reference to Artificial Intelligence, machine learning, or automated systems. The Act does not define these technologies or outline their scope, resulting in significant ambiguity in legal interpretation. Without clear definitions, it becomes difficult for courts and regulators to apply existing provisions to AI-driven activities, leading to inconsistent and uncertain outcomes.[11]

[8] *European Commission, White Paper on Artificial Intelligence (2020).*
[9] *Information Technology Act, 2000, Preamble.*
[10] *Ministry of Electronics and Information Technology, Report of the Committee of Experts on Data Protection Framework for India (2018).*
[11] *NITI Aayog, National Strategy for Artificial Intelligence (2018).*

4.2 Lack of Accountability Mechanisms

AI systems often function autonomously, making decisions without direct human involvement. This creates challenges in assigning responsibility when harm occurs. The IT Act does not clearly address whether liability should rest with developers, users, or manufacturers of AI systems. This lack of clarity undermines accountability and weakens legal enforcement, especially in cases where AI decisions cause financial loss or personal harm.[12]

4.3 Data Protection Gaps

AI technologies depend heavily on vast amounts of data, including personal and sensitive information. However, the IT Act provides only limited protection for data privacy and lacks comprehensive regulation of data processing practices. It does not address issues such as data minimisation, consent standards, or algorithmic bias, where AI systems may produce discriminatory outcomes based on flawed datasets.[13]

4.4 No Regulation of Algorithmic Decision-Making

AI-driven decisions increasingly affect critical areas such as employment, credit evaluation, and criminal justice. Despite this, the IT Act does not mandate transparency or explainability in algorithmic processes. Individuals affected by automated decisions are not granted a clear right to challenge or seek justification for such outcomes, raising concerns about fairness and due process.[14]

4.5 Inadequate Cybersecurity Framework

AI systems are particularly vulnerable to sophisticated threats such as data poisoning and adversarial attacks, where malicious actors manipulate inputs to influence outcomes. The IT Act primarily addresses conventional cyber threats and does not provide specific safeguards against these advanced AI-related vulnerabilities, leaving critical systems exposed.[5]

4.6 Jurisdictional Challenges

AI technologies often operate across national boundaries, involving data flows and platforms that span multiple jurisdictions. The IT Act has limited extraterritorial reach and struggles to regulate global AI companies effectively. This creates enforcement challenges and allows regulatory gaps to persist in cross-border contexts.[15]

In sum, the IT Act, 2000 lacks the conceptual depth and regulatory mechanisms required to govern AI technologies effectively, highlighting the urgent need for a modern, comprehensive legal framework.

Emerging Challenges Posed by AI

The rapid integration of Artificial Intelligence into governance, commerce, and daily life has introduced a range of complex challenges that extend beyond technological concerns into the realms of ethics, constitutional rights, and criminal law. These challenges highlight the urgent need for a nuanced legal and regulatory response.

5.1 Ethical Concerns

One of the most pressing issues associated with AI is the presence of bias in algorithms. AI systems are trained on large datasets, and if these datasets reflect existing social prejudices or inequalities, the resulting outputs may perpetuate or even amplify such biases. For instance, biased algorithms in hiring or lending systems can unfairly disadvantage certain groups, undermining principles of fairness and

[12] *Ryan Calo, "Robotics and the Lessons of Cyberlaw," (2015) 103 California Law Review 513.*
[13] *Justice B.N. Srikrishna Committee, Report on Data Protection Framework for India (2018).*
[14] *European Commission, White Paper on Artificial Intelligence (2020).*
[15] *Anupam Chander, "How Law Made Silicon Valley," (2017) Emory Law Journal.*

justice.[16]Additionally, there is a growing concern regarding the lack of fairness and inclusivity in AI systems. Many AI models are developed without adequate representation of diverse populations, leading to outcomes that may not be universally applicable or equitable. This raises ethical questions about whether AI technologies truly serve the interests of all sections of society or reinforce existing disparities.[17]

5.2 Impact on Fundamental Rights

The deployment of AI also poses significant risks to fundamental rights. The right to privacy, recognized as a fundamental right in Justice K.S. Puttaswamy v. Union of India, is particularly vulnerable, as AI systems rely heavily on the collection and processing of personal data, often without explicit or informed consent.[18]Moreover, AI-driven decisions may infringe upon the right to equality under Article 14 of the Constitution of India. If algorithms produce discriminatory outcomes, individuals may be subjected to unequal treatment without clear justification or recourse. The opacity of AI systems further complicates the ability to challenge such violations effectively.[19]

5.3 Criminal Liability Issues

AI also raises novel questions in the domain of criminal law. A key issue is determining who should be held responsible for crimes involving AI systems. When an autonomous system causes harm, it becomes difficult to attribute liability to a specific individual, whether it be the developer, operator, or user.[20]Another debated question is whether AI systems themselves can be granted legal personality. While some scholars argue for limited recognition to address accountability gaps, others caution that such an approach may undermine established legal principles that are premised on human intent and responsibility. These emerging challenges demonstrate that AI is not merely a technological issue but a legal and ethical one, requiring comprehensive reforms to ensure that innovation does not come at the cost of justice and fundamental rights.

Comparative International Frameworks

The regulation of Artificial Intelligence has become a global priority, with different jurisdictions adopting varied approaches based on their legal traditions, policy objectives, and technological capacities. A comparative analysis of these frameworks provides valuable insights for India in designing its own regulatory model.

6.1 European Union

The European Union has emerged as a global leader in AI regulation through its proposed AI Act, which adopts a risk-based approach. Under this framework, AI systems are classified into categories such as unacceptable risk, high risk, limited risk, and minimal risk. High-risk systems—such as those used in healthcare, law enforcement, and critical infrastructure—are subject to stringent compliance requirements, including rigorous testing, documentation, and human oversight.[21]A key feature of the EU approach is its strong emphasis on transparency and accountability. Developers are required to ensure explainability of AI systems, maintain detailed records, and provide users with clear information about how decisions are made. This framework aims to protect fundamental rights while fostering trust in AI technologies.

[16] *Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact," (2016) 104 California Law Review 671.*
[17] *Kate Crawford, Atlas of AI (Yale University Press, 2021).*
[18] *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*
[19] *Constitution of India, art. 14.*
[20] *Gabriel Hallevy, When Robots Kill: Artificial Intelligence under Criminal Law (Northeastern University Press, 2013).*
[21] *European Commission, Proposal for a Regulation on Artificial Intelligence (AI Act), 2021.*

6.2 United States

In contrast, the United States follows a more sector-specific and decentralized approach to AI regulation. Instead of a comprehensive federal law, regulatory oversight is distributed across various agencies depending on the sector, such as healthcare, finance, and consumer protection.[22]The U.S. model places significant emphasis on innovation and self-regulation, encouraging private companies to develop ethical guidelines and best practices. While this approach promotes technological advancement and flexibility, it has been criticised for lacking uniform standards and enforceable accountability mechanisms.[23]

6.3 China

China adopts a markedly different strategy characterized by strict state control over AI deployment. The government has introduced regulations requiring mandatory algorithm registration, particularly for recommendation systems and deep synthesis technologies.[24]China's framework prioritizes national security, social stability, and state oversight, with stringent compliance obligations for companies operating in the AI sector. While this ensures greater control and monitoring, it raises concerns regarding privacy and freedom of expression.[25]

Suggestions for India

India can draw important lessons from these diverse approaches. A risk-based regulatory model, similar to the EU, would allow differentiated regulation based on the potential harm of AI systems. At the same time, India should ensure transparency and accountability to protect individual rights. Finally, it must strike a careful balance between innovation and regulation, adopting flexible policies that encourage technological growth while safeguarding ethical and constitutional values.

Recommendations

Introduction of AI-Specific Legislation

- Enact a comprehensive and dedicated AI law that clearly defines Artificial Intelligence, machine learning, and automated decision-making systems to remove ambiguity in legal interpretation.
- Establish a clear scope of application, covering both public and private sector use of AI technologies.
- Incorporate ethical principles such as fairness, non-discrimination, transparency, and human oversight as legally enforceable standards rather than voluntary guidelines.
- Provide a structured regulatory framework for high-risk AI applications, especially in sectors like healthcare, finance, and criminal justice.

Strengthening Data Protection Framework

- Align India's data protection regime with global standards such as GDPR-like principles of accountability and user rights.
- Ensure informed and explicit consent for data collection and processing, particularly where AI systems rely on personal data.
- Introduce the principle of data minimization, limiting data collection to what is strictly necessary.
- Address algorithmic bias by mandating quality and diversity standards in datasets used for training AI systems.

[22] *U.S. National Institute of Standards and Technology (NIST), AI Risk Management Framework (2023).*
[23] *Andrew Tutt, "An FDA for Algorithms," (2017) 69 Administrative Law Review 83.*
[24] *Cyberspace Administration of China, Provisions on the Administration of Algorithmic Recommendation Services (2022).*
[25] *Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control," (2018).*

Establishment of Regulatory Authority

- Create an independent AI regulatory authority with technical expertise and legal powers.
- Empower the authority to monitor, audit, and certify AI systems, especially high-risk applications.
- Grant enforcement powers, including penalties, suspension of AI systems, and compliance orders.
- Facilitate coordination between government agencies, private stakeholders, and research institutions.

Algorithmic Transparency and Accountability

- Mandate disclosure obligations for organizations deploying AI systems, including information about how decisions are made.
- Introduce a legally enforceable "right to explanation", allowing individuals to understand automated decisions affecting them.
- Require regular audits and impact assessments of AI systems to ensure fairness and accountability.
- Promote human-in-the-loop mechanisms to oversee critical AI decisions.

Liability Framework

- Establish a clear allocation of responsibility among developers, deployers, and users of AI systems.
- Introduce strict liability for high-risk AI systems, ensuring compensation without requiring proof of fault.
- Develop product liability standards for AI-based technologies.
- Provide mechanisms for insurance and risk-sharing models to address AI-related damages.

International Cooperation

- Develop cross-border regulatory frameworks to address the global nature of AI technologies.
- Engage in international collaborations and treaties for harmonized AI governance.
- Adopt best practices from global models while tailoring them to India's socio-economic context.
- Facilitate data-sharing agreements with safeguards for privacy and security.
- Amend the Information Technology Act, 2000 to incorporate AI-specific definitions and regulatory provisions.
- Enact a comprehensive AI legislation addressing ethical, legal, and technical aspects.
- Transform ethical AI principles into binding legal obligations.
- Establish a National AI Regulatory Authority with strong oversight and enforcement powers.
- Ensure algorithmic transparency, explainability, and accountability across all AI applications.
- Adopt a risk-based regulatory approach, similar to international best practices, particularly the European model.
- Strengthen cybersecurity laws to address emerging AI-specific threats such as adversarial attacks and data manipulation.

These recommendations collectively aim to create a balanced legal framework that promotes innovation while ensuring accountability, protection of fundamental rights, and long-term public trust in AI systems.

Conclusion

The Information Technology Act, 2000 was undoubtedly a landmark legislation at the time of its enactment, laying the foundation for India's digital legal framework and enabling the growth of e-commerce and cyber governance. However, the rapid evolution of technology—particularly the emergence of Artificial Intelligence—has exposed the limitations of this law. The IT Act was designed to address conventional cyber issues such as hacking, data breaches, and electronic transactions, but it does

not possess the conceptual depth or regulatory mechanisms required to deal with the complexities of AI-driven systems.

Artificial Intelligence introduces fundamentally new challenges, including autonomous decision-making, algorithmic opacity, and data-intensive operations, which cannot be adequately governed by existing provisions. The absence of clear definitions, accountability structures, and safeguards against bias and discrimination creates significant legal uncertainty. Moreover, the increasing use of AI in sensitive domains such as healthcare, finance, and criminal justice raises serious concerns about the protection of fundamental rights, including privacy and equality. Without proper regulation, AI systems may operate in ways that are opaque, unaccountable, and potentially harmful.

In this context, it is imperative for India to adopt a forward-looking and adaptive legal approach. Reforming the existing framework, or introducing a dedicated AI legislation, is essential to bridge the gap between law and technology. Such a framework must strike a careful balance between fostering innovation and ensuring accountability. It should incorporate principles of transparency, fairness, and human oversight, while also addressing issues of liability and data protection.

Ultimately, a comprehensive and robust regulatory regime for AI is crucial not only for supporting technological advancement but also for building public trust and safeguarding democratic values in an increasingly automated world.

Bibliography

I. Books

1. Jain, Ashok K., Cyber Laws in India (LexisNexis, Latest Edition).
2. Reed, Chris, Internet Law: Text and Materials (Cambridge University Press, Latest Edition).
3. Russell, Stuart & Norvig, Peter, Artificial Intelligence: A Modern Approach (3rd ed., Pearson, 2010).
4. Abbott, Ryan, The Reasonable Robot: Artificial Intelligence and the Law (Cambridge University Press, 2020).
5. Hallevy, Gabriel, When Robots Kill: Artificial Intelligence under Criminal Law (Northeastern University Press, 2013).

II. Articles & Journal Publications

1. Barocas, Solon & Selbst, Andrew D., “Big Data’s Disparate Impact,” (2016) 104 California Law Review 671.
2. Tutt, Andrew, “An FDA for Algorithms,” (2017) 69 Administrative Law Review 83.
3. “Artificial Intelligence and Legal Liability,” Harvard Law Review (Recent Issue).
4. “Regulating AI: Global Perspectives,” Oxford Journal of Legal Studies (Recent Issue).
5. Calo, Ryan, “Robotics and the Lessons of Cyberlaw,” (2015) 103 California Law Review 513.

III. Legislation

1. Information Technology Act, 2000 (Act No. 21 of 2000).
2. Information Technology (Amendment) Act, 2008.
3. Digital Personal Data Protection Act, 2023.
4. Constitution of India, 1950 (especially Articles 14 and 21).

IV. Reports & Policy Documents

1. NITI Aayog, National Strategy for Artificial Intelligence (2018).
2. NITI Aayog, Responsible AI for All: Strategy for India (2021).
3. Justice B.N. Srikrishna Committee, Report on Data Protection Framework for India (2018).

4. European Commission, Proposal for a Regulation on Artificial Intelligence (AI Act) (2021).
5. European Commission, White Paper on Artificial Intelligence (2020).
6. U.S. National Institute of Standards and Technology (NIST), AI Risk Management Framework (2023).

V. Case Laws

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

VI. Online Sources

1. Ministry of Electronics and Information Technology (MeitY), Government of India – Official Reports and Notifications.
2. European Commission – AI Policy and Legislative Updates.
3. OECD AI Policy Observatory.