REGULATING ARTIFICIAL INTELLIGENCE AND LEGAL IMPLICATIONS: AN OVERVIEW

Yafrin Ramana, Advocate (Punjab and Haryana High Court), Punjab, India

ABSTRACT

Artificial Intelligence (AI) is a transformative technology that permeates our lives in numerous ways, performing tasks that, until recently, could only be performed by a human with specialised knowledge, training, or a government-issued license. AI is now widely used across sectors such as healthcare, finance, education, transportation, manufacturing, and public administration and is an unavoidable entity in today's world. The potential for further rapid advances in AI technology has prompted expressions of alarm from many quarters, including some calls for government regulation of AI development and restrictions on AI operation.[1]

Advancements in technology often calls for the government to regulate new technologies, this is not a new phenomena, it is done to provide a guideline for adequate use and to foresee the potential misuse. However, the rise of AI has so far occurred unregulated, with the exception of a few international states there have been no courts to concretely answer who is to be held legally liable if AI causes harm. Traditional regulatory approaches may not adequately address the unique characteristics of AI, including autonomy, adaptability, opacity, and rapid evolution. Moreover, regulation is met with difficulty at the primary stage, defining what **"**artificial intelligence" means.

The main objectives of this study are: *Why AI should be regulated* and *the interplay between AI and Law.* The paper discusses the legal implications, regulatory challenges and protection of legal right of humans. Finally, the study will attempt to offer a proposed framework for AI regulation.

Keywords: Artificial Intelligence, Regulation of Artificial Intelligences and Challenges, Artificial Intelligence and Law, Legal Implications, Human Rights, Legal Liability.

1 John Frank Weaver, We Need to Pass Legislation on Artificial Intelligence Early and Often, Slate (available at: http://www.slate.com/blogs/future_tense/2014/09/12/we_need_to_pass_artificial_intelligence_laws_early_and_often.html; Perri 6, Ethics, Regulation and the New Artificial Intelligence, Part I: Accountability and Power, *4 Info., Comm & Soc y 199, 203 (2001).*

1. Introduction

The rapid growth of AI has altered the relationship between technology and society and presents both practical and conceptual challenges for the legal system. Many of the practical challenges stem from the manner in which AI is researched and developed and from the basic problem of controlling the actions of autonomous machines.[2] The major challenges arise from the difficulties in assigning moral and legal responsibility for harm caused by autonomous machines, and from the puzzle of defining what, exactly, artificial intelligence means.[3]

AI is different from other technologies, and is considered transformative as it has changed the way the world works. Today, we are more dependent on AI than we realise, it is omnipresent. AI systems assist doctors in diagnosing diseases, recommend financial decisions, power autonomous vehicles, facilitate online transactions, generate creative content, and support decision-making in both the public and private sectors. As these systems become increasingly sophisticated, they are no longer viewed merely as technological tools but as systems capable of making decisions with varying degrees of autonomy. It has significant impact on both, humans and law.

Law plays an important role in regulating technology to safeguard the society as technologies move fast, they may outpace law leading to future problems which we may not be able to tackle. At present there is no universally accepted international framework for AI. India, despite rapidly adopting AI across multiple sectors, does not presently have a comprehensive legislation specifically regulating AI. Instead, AI-related issues are addressed through existing statutes such as the *Information Technology Act, 2000,*[4] which is the online act concerning technology and the *Digital Personal Data Protection Act, 2023*,[5] which is insufficient for the regulation. These laws provide partial protection, they do not comprehensively address questions relating to liability, accountability, transparency, or autonomous decision-making.

An additional challenge lies in defining artificial intelligence itself. There is no universally accepted legal definition of AI, and the technology continues to evolve at a pace that frequently outstrips legislative responses.[6] The absence of conceptual clarity makes it difficult to

[2] David C. Vladeck, Machines Without Principals: *Liability Rules and Artificial Intelligence,* 89 Wash. L. Rev. 117, 121 (2014).
[3] *Harvard Journal of Law & Technology, Vol. 29, No. 2 (Spring 2016).*
[4] *Information Technology Act, 2000.*
[5] *Digital Personal Data Protection Act, 2023.*
[6] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

determine the scope of regulation, identify responsible actors, and develop uniform standards capable of balancing innovation with public interest.

The present paper examines the relationship between artificial intelligence and law by analysing the legal implications arising from the increasing use of AI, the regulatory challenges faced by lawmakers, and the need to safeguard the legal rights of individuals. It further evaluates existing regulatory approaches and proposes a balanced legal framework that promotes innovation while ensuring accountability, public safety, and the protection of fundamental rights.

1.2 Objectives of the Study

1. To analyse if AI should be regulated.
2. To recognise the interplay of AI and Law.
3. To identify the legal and regulatory challenges arising from the autonomous and evolving nature of Artificial Intelligence, including issues relating to accountability, transparency, and attribution of liability.
4. To examine the implications of Artificial Intelligence on fundamental legal rights, including privacy, equality, autonomy, and access to justice.
5. To propose a balanced legal framework and effective legal protection against harms arising from the use of Artificial Intelligence.

2. Understanding Artificial Intelligence

2.1 What is AI?

The term "Artificial Intelligence" was coined by American computer scientist John McCarthy in 1955 as part of a proposal for the historic 1956 Dartmouth Summer Research Project on Artificial Intelligence, he deliberately coined the new term to separate this emerging field of computer science from the study of "cybernetics" and to emphasise that machines could be engineered to simulate human intelligence.[7]

[7] History of Artificial Intelligence, *Wikipedia, https://en.wikipedia.org/wiki/History_of_artificial_intelligence (last visited July 2, 2026).*

McCarthy stated that there is no "solid definition of intelligence that doesn't depend on relating it to human intelligence" because "we cannot yet characterise in general what kinds of computational procedures we want to call intelligent."[8] Definitions of intelligence thus vary widely and focus on myriad interconnected human characteristics that are themselves difficult to define, including consciousness, self-awareness, language use, the ability to learn, the ability to abstract, the ability to adapt, and the ability to reason.[9]

McCarthy defined intelligence as "the computational part of the ability to achieve goals in the world" and AI as "the science and engineering of making intelligent machines, especially intelligent computer programs."[10] However, if one aims to define AI using a goal-oriented lens, the definition would be ever-changing. Consequently, a goal-oriented definition does not provide a working definition of AI for regulatory purposes.

Early approaches to defining AI often tied the concept of intelligence to the ability to perform particular intellectual tasks. As a result, concepts have shifted over time with advancement in technology that allows computers to perform tasks which previously were thought to be the hallmark of intelligence. Chess once was one such hallmark, but computers could play a passable game of chess by the 1960s[11] and could defeat the best human player in the world by 1997.[12]

Today's AI goals are different, they are designed for a broad spectrum of objectives, including pattern recognition, probabilistic inference, logical reasoning, optimisation, autonomous decision-making, and machine learning.. AI infiltrates all aspects of human life thus, finding a definition is to put it in a box knowing that it is not limited. Accordingly, arriving at a universally accepted definition remains elusive, making context-specific definitions more useful for legal and regulatory analysis.

For the purposes of this paper, **Artificial Intelligence** may be understood as a computational system that perceives information, learns or applies programmed logic to that information, and autonomously or semi-autonomously produces decisions, predictions, or actions intended to

[8] John McCarthy, *What Is Artificial Intelligence? 2–3* (Jul 2, 2026), https://www-formal.stanford.edu/jmc/whatisai.pdf.
[9] David Premack, Intelligence in Ape and Man (1976).
[10] John McCarthy, What Is Artificial Intelligence?
[11] NILS J. NILSSON, THE QUEST FOR ARTIFICIAL INTELLIGENCE 194 (2010).
[12] BRUCE PANDOLFINI, KASPAROV AND DEEP BLUE: THE HISTORIC CHESS MATCH BETWEEN MAN AND MACHINE 7–8 (1997).

achieve predefined objectives with minimal ongoing human intervention.

2.2 Characteristics of Artificial Intelligence

Artificial Intelligence possesses a number of defining characteristics that distinguish it from traditional software systems. While conventional computer programs operate strictly according to predetermined instructions, AI systems are capable of analysing data, recognising patterns, learning from experience, and making decisions with varying degrees of autonomy. These characteristics have become increasingly significant in legal and regulatory discourse because they influence issues relating to accountability, transparency, liability, and governance. The goal-oriented nature distinguishes AI from conventional software that merely executes static instructions.[13]

Learning Capability:

A defining characteristic of AI is its ability to learn from data rather than relying solely on explicitly programmed instructions. Through machine learning techniques, AI systems identify patterns within datasets and improve their performance over time without requiring continuous human intervention. This adaptive capability enables AI to respond to new information and changing environments more effectively than traditional software.[14]

Autonomy:

systems can perform tasks autonomously by making decisions or recommendations based on predefined objectives. The degree of autonomy varies depending on the application, ranging from decision-support systems that assist human users to fully autonomous systems capable of operating with minimal human oversight. Modern regulatory frameworks increasingly classify AI according to the level of human involvement in decision-making.[15]

Reasoning and Decision-Making:

AI systems utilise computational models to evaluate information, draw logical inferences, and generate outputs aimed at achieving specified objectives. Unlike conventional software that follows fixed procedural rules, AI systems can process large volumes of structured and

[13] John McCarthy, What Is Artificial Intelligence? (Stanford University, 2007) 2–4.
[14] Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (4th edn, Pearson 2021) 22–31.
[15] European Parliament and Council, Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) [2024] OJ L, art 3.

unstructured data to support complex decision-making processes. This characteristic has contributed to AI's widespread use in healthcare, finance, transportation, and public administration.[16]

Pattern Recognition:

One of AI's most significant capabilities is recognising patterns within large datasets that may not be immediately apparent to human observers. Pattern recognition underpins technologies such as facial recognition, fraud detection, speech recognition, and predictive analytics. Advances in deep learning have substantially enhanced the accuracy and efficiency of pattern recognition systems.[17]

Data Dependency:

The effectiveness of AI depends heavily upon the availability, quality, and representativeness of data. Since AI systems derive insights from training data, biased, incomplete, or inaccurate datasets may produce discriminatory or unreliable outcomes. Consequently, data governance has become a central concern in AI regulation and ethical governance frameworks.[18]

In summary, these characteristics demonstrate that AI is not defined solely by computational capability but by its capacity to learn, adapt, reason, and perform tasks with varying degrees of autonomy. These features also explain why AI presents unique legal challenges concerning accountability, transparency, fairness, privacy, and regulatory governance.

3. Role of Artificial Intelligence in Law

Advancements in AI has led to a widely accepted changes in the manner that we carry out daily activities. The legal profession is no exception to this transformation. Legal practitioners are increasingly utilising various types of AI and data analytics tools and smart virtual assistants to enhance their work efficiency, streamline tasks, and improve client services.[19]

It's time for us to accept that Artificial Intelligence has the potential to transform the way

[16] OECD, OECD Recommendation of the Council on Artificial Intelligence (OECD Legal Instruments, 2019).
[17] Ian Goodfellow, Yoshua Bengio and Aaron Courville, Deep Learning (MIT Press 2016) chs 8–9.
[18] OECD, OECD Artificial Intelligence Principles (2019); European Commission, Ethics Guidelines for Trustworthy AI (2019).
[19] Daniel Linna Jr and Wendy Muchman, 'Ethical Obligations to Protect Client Data when Building Artificial Intelligence Tools: Wigmore Meets AI '(American Bar Association, 2020).

lawyers currently work and the way law is viewed in India. As stated by Justice D.Y. Chandrachud, "technology is relevant insofar as it fosters efficiency, transparency, and objectivity in public government. AI is present to provide a facilitative tool to judges in order to recheck or evaluate the work, the process, and the judgments."

The AI Task Force Report was the first phase in India's Artificial Intelligence framework, and it was used to examine artificial intelligence in depth. The Ministry of Commerce and Industry established this task force, which is led by N. Chandrasekaran, Chairman of Tata Sons, to examine the financial benefits of AI and determine how it can benefit India.[20] The Task-force stated its vision "To embed AI in our Economic, Political and Legal thought processes so that there is the systematic capability to support the goal of India becoming one of the leaders of AI-rich economies".[21]

Indian law is vast and ever evolving, with numerous statutes, amendments, and landmark judicial pronouncements shaping its interpretation regularly. Keeping pace with these developments is a significant challenge for legal practitioners, particularly given the nuanced nature of Indian jurisprudence, which often requires manual research and analysis. In this context, the integration of AI into the legal profession has become increasingly important. AI can assist advocates by tracking legislative changes, monitoring recent judgments, and streamlining legal research, enabling them to stay up to date with the latest legal developments. By reducing the time spent on repetitive research tasks, AI allows advocates to focus more effectively on legal strategy, client representation, and the ultimate objective of delivering justice.

However, to be able to use AI, a regulation is needed to understand the manner in which it can be used.

4. Artificial Intelligence Regulation in India

4.1 Existing Legal Framework

India has not enacted a dedicated legislation governing Artificial Intelligence. Instead, India

[20] https://indianexpress.com/article/technology/tech-news-technology/task-force-set-up-to-study-ai-application-in-military-5049568/
[21] https://legaldesire.com/scope-of-artificial-intelligence-in-law/#_ftn1

has consciously adopted a technology-neutral and sectoral approach, regulating AI indirectly through existing statutes, executive policies, and governmental guidelines rather than through a single comprehensive enactment.

This approach reflects the Government's attempt to encourage innovation while simultaneously relying upon existing legal mechanisms to address issues arising from the deployment of AI systems. Although such flexibility allows the law to accommodate technological developments without frequent legislative amendments, it also creates uncertainty regarding accountability, liability, transparency, and governance of autonomous AI systems.

Consequently, the present regulatory framework primarily addresses the consequences arising from the use of AI rather than regulating the technology itself. This approach becomes particularly significant where autonomous systems make decisions capable of causing harm.

4.2 Information Technology Act, 2000

The Information Technology Act, 2000, remains India's principal legislation governing electronic transactions, cyber offences, intermediary liability, and digital communications. Although enacted long before the emergence of modern Artificial Intelligence, many of its provisions continue to apply indirectly to AI-enabled activities.[22]

For instance, offences relating to identity theft, cheating by personation using computer resources, unauthorised access, hacking, publication of obscene material, and cyber fraud may equally apply where such offences are committed through AI-enabled technologies. Similarly, intermediaries deploying AI-based platforms continue to be governed by the due diligence obligations prescribed under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which explicitly mandate the labelling and restriction of AI generated content under 2026 amendments.[23]

However, the Act was drafted at a time when software largely functioned as a passive technological tool. Contemporary AI systems are capable of generating original content, learning from user interactions, adapting their behaviour, and making autonomous

[22] Information Technology Act, 2000.
[23] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

recommendations. These characteristics create situations that were never contemplated by the legislature in 2000.

Accordingly, while the Information Technology Act regulates unlawful digital conduct facilitated through AI, it does not directly regulate the development, deployment, accountability, or autonomous functioning of AI systems themselves.

4.3 Digital Personal Data Protection Act, 2023

Artificial Intelligence is fundamentally dependent upon data. Machine learning models derive their capabilities by processing enormous quantities of information, much of which consists of personal data. Consequently, data protection has become one of the central pillars of AI governance.

The Digital Personal Data Protection Act, 2023 establishes India's first comprehensive legislative framework governing the processing of digital personal data.[24] The Act recognises the rights of individuals over their personal data while imposing corresponding obligations upon Data Fiduciaries responsible for processing such information.

The legislation introduces principles relating to lawful consent, purpose limitation, data minimisation, storage limitation, security safeguards, and grievance redressal. These safeguards are particularly relevant where AI systems rely upon personal information for training, profiling, prediction, or automated decision-making.

Despite these advancements, the Act does not directly regulate Artificial Intelligence. It focuses primarily on the collection and processing of personal data rather than addressing broader issues such as algorithmic transparency, explainability, autonomous decision-making, or allocation of legal responsibility when AI systems cause harm.

Consequently, while the Digital Personal Data Protection Act constitutes an important component of AI governance, it cannot be regarded as a comprehensive regulatory framework governing Artificial Intelligence.

[24] Digital Personal Data Protection Act, 2023.

4.4 Government Policy Initiative

Recognising the transformative potential of Artificial Intelligence, the Government of India has adopted several policy initiatives aimed at encouraging responsible innovation.

One of the earliest comprehensive policy documents was the National Strategy for Artificial Intelligence, published by NITI Aayog in 2018 under the theme "AI for All."[25] Rather than focusing exclusively upon regulation, the Strategy sought to identify sectors where AI could contribute significantly to national development, including healthcare, agriculture, education, smart mobility, and smart cities.

The Strategy emphasised that India should pursue a balanced approach that simultaneously promotes innovation and safeguards ethical values such as inclusivity, privacy, fairness, transparency, and accountability.

More recently, the Government launched the *IndiaAI Mission*, which aims to strengthen India's AI ecosystem through investments in computing infrastructure, datasets, research, skill development, startup support, and responsible AI innovation.[26]The Mission reflects India's objective of becoming a global leader in trustworthy and inclusive Artificial Intelligence.

Although these initiatives demonstrate a strong governmental commitment towards AI development, they remain policy instruments rather than binding legislation and therefore possess limited enforceability.

5. Comparative Jurisprudence on the Regulation of Artificial Intelligence

The rapid expansion of Artificial Intelligence has compelled governments across the world to reconsider whether traditional legal frameworks are capable of regulating autonomous technologies.[27] Although there is broad international consensus that AI requires regulatory oversight, there remains significant divergence regarding the appropriate model of regulation.[28] While some jurisdictions have adopted comprehensive legislation specifically governing AI,

[25] National Institution for Transforming India, National Strategy for Artificial Intelligence (June 2018).
[26] IndiaAI Mission, Ministry of Electronics and Information Technology, Government of India.
[27] OECD, Recommendation of the Council on Artificial Intelligence (2019).
[28] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

others continue to regulate the technology indirectly through existing statutory frameworks.[29]

This divergence reflects differing policy priorities. The European Union has emphasised protection of fundamental rights and adopted a precautionary, risk-based regulatory framework.[30] The United States has largely favoured innovation through sector-specific regulation, whereas China has adopted a model characterised by extensive governmental oversight and mandatory compliance requirements. India's present approach falls somewhere between these models, relying upon existing legislation and executive policies while avoiding comprehensive AI-specific legislation.

A comparative analysis is particularly valuable because AI operates across territorial boundaries. Lessons drawn from foreign jurisdictions can assist India in identifying regulatory mechanisms that balance innovation with accountability without unnecessarily hindering technological development.

5.1 European Union: A Risk-Based Regulatory Model

The European Union has emerged as the global leader in AI regulation through the enactment of the Artificial Intelligence Act.[31] Unlike earlier regulatory initiatives that addressed isolated concerns such as privacy or cybersecurity, the AI Act establishes a comprehensive legal framework specifically governing Artificial Intelligence.

Rather than treating every AI system alike, the legislation classifies AI applications according to the level of risk they pose. AI systems presenting unacceptable risks, such as certain forms of social scoring or manipulative AI that exploits vulnerable persons, are prohibited altogether.[32] High-risk systems, including those deployed in healthcare, law enforcement, education, employment, and critical infrastructure, remain permissible but are subjected to extensive compliance obligations relating to transparency, human oversight, data governance, documentation, and risk management.[33]

This classification reflects an important regulatory principle: not all AI systems require identical levels of legal intervention. Instead, regulatory obligations should correspond to the

[29] Regulation (EU) 2024/1689 (Artificial Intelligence Act).
[30] European Commission, Proposal for an Artificial Intelligence Act, COM(2021) 206 final.
[31] Regulation (EU) 2024/1689.
[32] AI Act, arts. 5–7.
[33] AI Act, arts. 8–27.

magnitude of potential harm. Such an approach enables innovation in low-risk sectors while ensuring stricter scrutiny where AI decisions directly affect life, liberty, health, employment, or other fundamental rights.

Another notable feature of the EU framework is its emphasis on accountability throughout the lifecycle of an AI system. Developers, deployers, importers, and distributors each bear defined legal obligations. Responsibility is therefore distributed according to the role played by each participant rather than being concentrated upon a single actor.

Despite these strengths, the European model has attracted criticism. Compliance requirements are often considered expensive and administratively burdensome, particularly for start-ups and small technology enterprises. Critics argue that excessive regulation may discourage innovation and slow technological development when compared to less restrictive jurisdictions.

Nevertheless, the EU AI Act represents the most comprehensive attempt to regulate AI through dedicated legislation and has become an influential reference point for policymakers across the world.

5.2 United States: Innovation Through Sectoral Regulation

Unlike the European Union, the United States has not enacted a single federal statute comprehensively regulating Artificial Intelligence.[34] Instead, regulation has developed through a combination of existing legislation, executive actions, sector-specific agencies, judicial decisions, and voluntary technical standards.[35]

This approach reflects the long-standing American preference for encouraging innovation while addressing risks as they emerge. Federal agencies regulate AI within their respective fields of competence. For example, healthcare AI falls within the jurisdiction of the Food and Drug Administration, financial algorithms are supervised through financial regulators, and competition-related issues may attract scrutiny from the Federal Trade Commission.

In recent years, the United States has also placed increasing emphasis on responsible AI development through the National Institute of Standards and Technology (NIST) AI Risk

[34] Executive Order No. 14110 (2023).
[35] Executive Order No. 14110.

Management Framework.[36] Although not legally binding, the framework encourages organisations to identify, assess, and mitigate AI-related risks through governance, transparency, validation, and continuous monitoring.

The American model demonstrates considerable regulatory flexibility. However, its fragmented nature may result in inconsistent standards across sectors and uncertainty regarding liability when AI systems operate across multiple regulatory domains.

5.3 China: State-Centred Regulation of Artificial Intelligence

China has adopted a significantly different regulatory philosophy. Rather than relying primarily upon market-led innovation, the Chinese framework combines rapid technological development with extensive governmental oversight.

Chinese regulations governing recommendation algorithms, deep synthesis technologies, and generative AI impose obligations relating to security assessments, content moderation, transparency, and compliance with national laws.[37] Developers are expected to implement mechanisms that reduce misinformation, unlawful content, and algorithmic manipulation before deployment.

This preventive approach allows regulators to intervene at an early stage of technological development. However, scholars have questioned whether extensive governmental control may affect freedom of expression, privacy, and innovation.

The Chinese model therefore demonstrates that strong regulation can coexist with rapid technological advancement, although it raises distinct constitutional and human rights concerns.

5.4 India's Position in Comparative Perspective

India has adopted neither the comprehensive legislative approach of the European Union nor the extensive administrative oversight observed in China. Instead, India presently regulates Artificial Intelligence indirectly through existing statutes, policy initiatives, and executive

[36] NIST AI RMF 1.0.
[37] Measures for Generative AI Services, arts. 4–12.

guidelines.[38]

This approach has several advantages. It allows policymakers to avoid premature legislation in a rapidly evolving field and reduces the risk of creating rigid statutory provisions that may quickly become obsolete. It also enables innovation by permitting AI development without imposing extensive compliance obligations during the technology's formative stages.

However, this flexibility comes at a cost. Unlike the European Union, India presently lacks statutory provisions governing high-risk AI systems, mandatory algorithmic transparency, independent auditing, explainability requirements, or clear allocation of legal responsibility between developers, deployers, users, and technology providers.

As AI systems increasingly influence healthcare, finance, employment, criminal justice, and public administration, these omissions may create uncertainty regarding accountability and public confidence.

5.5 Lessons for India

Comparative analysis suggests that no single jurisdiction has produced a perfect regulatory model. Each approach reflects different constitutional traditions, economic priorities, and policy objectives.

Nevertheless, certain principles emerge consistently across jurisdictions. First, AI regulation should distinguish between systems according to the level of risk they present rather than regulating all AI applications identically. Secondly, accountability should extend beyond end users and encompass developers, deployers, and organisations responsible for introducing AI into society. Thirdly, transparency and human oversight remain essential safeguards, particularly where AI decisions significantly affect legal rights.

India need not replicate any foreign framework in its entirety. Rather, it should adopt a regulatory model that reflects its own constitutional values while incorporating internationally recognised principles of fairness, accountability, transparency, and responsible innovation.

[38] NITI Aayog, AI For All (2018); MeitY AI Governance Guidelines (2025).

6. Criminal Liability of Artificial Intelligence

The increasing autonomy of Artificial Intelligence has exposed one of the most significant limitations of contemporary criminal law: its assumption that every criminal act originates from a human actor possessing intention, knowledge, or negligence.[39] Traditional criminal jurisprudence was developed around human behaviour, where liability is imposed only after establishing both the prohibited act (actus reus) and the accompanying guilty mind (mens rea).[40]

Unlike conventional software, they are capable of learning from data, adapting to changing circumstances, and producing outputs that may not have been specifically anticipated by their developers or users. Consequently, where harm results from an AI system, determining criminal responsibility becomes significantly more complex than in ordinary criminal cases.

The question is therefore no longer whether AI can cause harm, it undoubtedly can, but whether existing principles of criminal liability are capable of identifying an appropriate legal wrongdoer.

6.1 Can Artificial Intelligence Commit a Crime?

At present, the answer under Indian law is in the negative. Criminal liability attaches only to legal persons recognised by law. While corporations may, under certain circumstances, incur criminal liability, Artificial Intelligence itself possesses neither legal personality nor independent rights and obligations.[41]

Furthermore, AI lacks consciousness, moral agency, and the capacity to understand the legal consequences of its actions. Although advanced AI systems may generate decisions that appear intelligent, such outputs remain the product of computational processes rather than legal intention.

Accordingly, AI cannot presently be regarded as an offender capable of committing a crime in its own right. The more difficult legal question concerns the identification of the human actor who should bear responsibility for AI-generated harm.

[39] Andrew Ashworth & Jeremy Horder, Principles of Criminal Law (9th ed., Oxford University Press 2019).
[40] H.L.A. Hart, Punishment and Responsibility (2nd ed., Oxford University Press 2008).
[41] Iridium India Telecom Ltd. v. Motorola Inc., (2011) 1 SCC 74.

6.2 The Challenge of Mens Rea

One of the defining features of criminal liability is the requirement of a guilty mind. Depending upon the offence, this may consist of intention, knowledge, recklessness, or negligence.[42]

Artificial Intelligence does not possess consciousness or subjective awareness. It does not formulate intentions, appreciate legal consequences, or exercise moral judgment in the manner contemplated by criminal law. Even where AI appears to make autonomous decisions, those decisions arise from algorithms, training data, and computational models rather than conscious deliberation.

This creates a doctrinal gap. If the mental element cannot be attributed to AI, liability must necessarily be traced back to one or more human participants involved in designing, deploying, supervising, or operating the system.

However, this approach is not always straightforward. Modern AI systems often evolve through continuous learning, producing outcomes that were neither intended nor foreseeable by individual developers. Consequently, attributing *mens rea* to a particular individual may become increasingly difficult as AI autonomy expands.

6.3 The Problem of Actus Reus

Unlike the mental element, the physical element of an offence presents comparatively fewer conceptual difficulties. AI systems are capable of producing tangible consequences. An autonomous vehicle may collide with pedestrians, an AI-powered medical diagnostic system may recommend incorrect treatment, or an algorithm may facilitate financial fraud.

The difficulty lies not in identifying the prohibited act but in determining whose act it should legally be regarded as. Criminal law has traditionally treated technological instruments as extensions of human conduct. A firearm does not commit murder independently; responsibility rests with the individual who uses it.

Artificial Intelligence complicates this analogy because autonomous systems may generate outputs without direct human instruction at the moment the harm occurs. The causal chain

[42] K.D. Gaur, Textbook on Indian Penal Code (7th ed.).

therefore becomes distributed among developers, deployers, users, and the system itself.

6.4 Vicarious Liability: Can AI Be Compared to an Employee?

One possible analogy is the doctrine of vicarious liability, often expressed through the principle that an employer may be held liable for the acts of an employee committed during the course of employment.[43]

In *State of Rajasthan v. Vidhyawati*, the Supreme Court recognised that the State could be held liable for the negligent acts of its employee committed during the course of employment.[44] Although this principle has traditionally developed within civil law, it provides a useful conceptual framework for examining AI liability.

At first glance, an AI system appears analogous to an employee. Both perform assigned tasks, operate under delegated authority, and may cause harm while carrying out those functions. Consequently, it may appear reasonable to attribute liability to the developer, deployer, or organisation controlling the AI system.

However, the analogy quickly breaks down. An employee possesses independent judgment, legal capacity, and the ability to appreciate legal obligations. AI possesses none of these attributes. Conversely, AI systems may continuously modify their outputs through machine learning in ways that no human employee could. Treating AI simply as another employee therefore oversimplifies its legal character.

Accordingly, while vicarious liability offers useful guidance, it cannot by itself resolve the allocation of criminal responsibility for autonomous AI systems.

6.5 Strict Liability and Regulatory Offences

Given the evidentiary difficulties associated with proving *mens rea* in AI-related cases, some scholars have suggested greater reliance upon strict liability in carefully defined high-risk contexts.[45]

[43] Salmond, Law of Torts (21st ed.) (discussion on vicarious liability).
[44] State of Rajasthan v. Vidhyawati, AIR 1962 SC 933.
[45] See generally A.P. Simester et al., Simester and Sullivan's Criminal Law: Theory and Doctrine (7th ed., Hart Publishing 2019) (discussion of strict liability offences).

Under such a model, liability would arise upon proof that a prohibited consequence occurred, irrespective of subjective intention. Similar approaches already exist in areas involving inherently hazardous activities where public safety demands heightened standards of responsibility.

Such a framework may be particularly appropriate for AI deployed in healthcare, autonomous transportation, critical infrastructure, and public administration, where errors may produce irreversible consequences.

However, excessive reliance upon strict liability risks discouraging innovation and imposing disproportionate burdens upon developers acting with reasonable care. Accordingly, any such approach must be confined to narrowly defined categories of high-risk AI.

6.6 Towards a Shared Liability Model

The preceding analysis demonstrates that no single traditional doctrine adequately resolves the problem of AI-generated harm. Vicarious liability, corporate liability, and strict liability each address certain aspects of the problem while leaving significant gaps.

A more realistic solution may therefore lie in adopting a shared liability model. Under such a framework, responsibility would be allocated according to each participant's degree of control over the AI system. Developers may be liable for negligent design, deployers for unsafe implementation, users for foreseeable misuse, and organisations for failures of governance or supervision.

Such an approach better reflects the distributed nature of AI decision-making while preserving the fundamental principle that criminal liability should ultimately remain attributable to human actors rather than autonomous machines.

The law must evolve without abandoning its foundational principles. Rather than recognising AI as an independent offender, future legal frameworks should focus upon developing coherent standards for allocating responsibility among the human actors involved in the creation, deployment, and supervision of autonomous systems. Such an approach preserves accountability while acknowledging the technological realities of the twenty-first century.

7. Emerging Challenges in Attributing Criminal Liability to Artificial Intelligence

The preceding chapter examined the limitations of traditional principles of criminal liability when applied to Artificial Intelligence. While those challenges remain largely conceptual, recent developments demonstrate that they are no longer confined to academic debate. AI systems have already begun influencing decisions capable of affecting life, property, privacy, reputation and public safety. This chapter analyses selected real-world incidents involving Artificial Intelligence to illustrate the practical difficulties associated with identifying the legally responsible actor.

7.1 Autonomous Vehicles and Road Fatalities

One of the earliest incidents demonstrating the legal complexity of AI occurred in 2018 when an autonomous vehicle operated by Uber struck and killed a pedestrian during testing in Arizona, United States.[46] Investigations revealed that although the vehicle's sensors detected the pedestrian, the system failed to classify the object correctly and initiate timely braking.[47] The safety operator present inside the vehicle was subsequently prosecuted, while Uber entered into a civil settlement with the victim's family.[48]

The incident illustrates that autonomous decision-making frequently involves multiple participants. Responsibility may potentially lie with software developers, vehicle manufacturers, testing companies, safety operators or organisations responsible for supervision. Existing criminal law, however, generally seeks to identify one principal offender. Such an approach becomes increasingly difficult where harmful outcomes result from a combination of software design, machine learning, human oversight and organisational decision-making.The Uber incident therefore demonstrates that AI-related harm often emerges from distributed decision-making rather than the conduct of a single individual.

In legal literature, this dynamic creates what is known as a *"liability crumple zone."* Just as the crumple zone of a vehicle absorbs the impact of a crash, the human operator at the bottom of the technological loop absorbs the entire legal shock of a systemic failure, while the corporate

[46] National Transportation Safety Board (NTSB), *Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian,* Accident Report HAR-19/03 (2019).
[47] National Transportation Safety Board, Highway Accident Report: Uber Automated Vehicle Crash (2019).
[48] Yavapai County Attorney's Office, Investigation into the Uber Autonomous Vehicle Collision (2020).

and algorithmic structures that generated the risk remain largely insulated from penal sanctions.[49]

7.2 Artificial Intelligence in Healthcare

Artificial Intelligence is increasingly deployed in medical diagnosis, radiology, drug discovery and clinical decision-support systems. Such technologies have improved diagnostic efficiency and reduced administrative burdens upon healthcare professionals.[50]

Nevertheless, AI-assisted medical errors present significant legal concerns. If an AI diagnostic system incorrectly classifies a malignant tumour as benign, causing delayed treatment and death, determining criminal responsibility becomes exceptionally difficult. Should liability attach to the hospital relying upon the software, the physician accepting its recommendation, the software developer responsible for the algorithm, or the company that trained the model?

Indian law presently provides no comprehensive statutory framework addressing criminal liability arising from autonomous medical decision-making. Existing negligence principles remain applicable, yet they were developed in circumstances where professional judgment originated entirely from human actors.

While the National Medical Commission (NMC) mandates ethical boundaries for digital tools, active litigation relies on legacy negligence principles. However, these principles were developed under the assumption that professional judgment originates entirely from human actors. On the civil side, victims must look to *Section 82* of the *Consumer Protection Act, 2019*, to argue Product Liability defects against software developers, a framework poorly equipped to handle the evolving, non-deterministic nature of adaptive machine learning models.[51]

Accordingly, healthcare represents one of the sectors where AI regulation requires the greatest statutory clarity.

7.3 Deepfakes, AI-Generated Content and Online Harm

Generative Artificial Intelligence has significantly expanded the capacity to produce realistic images, audio recordings and videos that are indistinguishable from genuine content. While

[49] Elish, M. C., "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction,
[50] World Health Organization, Ethics and Governance of Artificial Intelligence for Health (2021).
[51] *Consumer Protection Act, 2019.*

these technologies possess legitimate applications in education, entertainment and accessibility, they have also facilitated new forms of cybercrime.

Deepfake technology has been used to create non-consensual intimate images, impersonate public officials, facilitate financial fraud and spread political misinformation.[52] Such conduct Such conduct falls within a dual web of prosecution under the Bharatiya Nyaya Sanhita (BNS), 2023 (such as Section 319 for cheating by personation) and the Information Technology Act, 2000.[53] However, the allocation of criminal responsibility remains deeply uncertain when harmful content is generated through publicly available, open-source AI systems.

The issue becomes particularly complex where AI platforms generate unlawful content in response to user prompts. Responsibility may potentially extend to the individual user, the developer of the foundation model, the company deploying the chatbot, or the platform hosting the service. Under India's Information Technology (Intermediary Guidelines) Rules, 2021 (as amended), hosting platforms face an explicit compliance mandate to actively detect, filter, and label Synthetically Generated Information (SGI).[54] Failure to meet these due diligence standards results in the forfeiture of their statutory statutory "safe harbor" protection, demonstrating a shift toward holding platforms vicariously responsible for the containment of algorithmic harms.

Existing legal frameworks provide limited guidance regarding how responsibility should be distributed among these participants.

7.4 Algorithmic Bias and Discriminatory Decision-Making

Artificial Intelligence systems derive their predictions from historical datasets. Where those datasets contain existing social or institutional biases, AI systems may reproduce or even amplify discriminatory outcomes.[55]

A frequently cited example is the COMPAS algorithm used in parts of the United States to assist judicial risk assessments. Academic research suggested that the system

[52] Interpol, Global Trend Report on Cybercrime (2023) (discussing deepfakes and AI-enabled cybercrime).
[53] Bharatiya Nyaya Sanhita (BNS), 2023 and the Information Technology Act, 2000.
[54] Information Technology (Intermediary Guidelines) Rules, 2021 (as amended)
[55] Organisation for Economic Co-operation and Development, OECD AI Principles (2019).

disproportionately classified certain racial groups as presenting a higher risk of reoffending, thereby raising concerns regarding fairness and equality before the law.[7]

Although such systems are not presently employed in India's criminal justice system on a comparable scale, increasing reliance upon automated decision-making in governance raises similar concerns. Bias embedded within AI systems may indirectly influence recruitment, financial lending, healthcare access and policing.

From a legal perspective, discriminatory AI challenges traditional paradigms because the resulting harm does not arise from intentional discrimination (*animus*) by any identifiable human individual, but from systemic patterns embedded within historical training data. When deployed by the State, this automated discrimination triggers violations of Articles 14 and 15 of the Constitution of India, yet existing administrative law lacks the procedural tools required to audit or remedy "black-box" algorithmic bias.[56]

7.5 Conversational Artificial Intelligence and Harmful Outputs

The emergence of large language models and conversational AI systems has transformed public interaction with Artificial Intelligence. These systems are capable of producing sophisticated responses, generating software code, drafting legal documents and creating multimedia content. At the same time, they have generated renewed concerns regarding misinformation, explicit content and harmful advice.

Recent public controversies involving conversational AI platforms have demonstrated that AI systems may produce inaccurate legal guidance, offensive responses or explicit material under certain circumstances. These incidents raise an important legal question: where harmful content originates from probabilistic text generation rather than deliberate human intention, who should bear legal responsibility?

Unlike traditional publications, conversational AI continuously generates new outputs depending upon user interaction. Harm therefore results not from a pre-existing publication but from an ongoing interaction between the user and the AI system. This characteristic

[56] Art 14 and 15, Constitution of India

complicates the application of conventional criminal doctrines developed for human authorship.

7.6 Artificial Intelligence and Financial Crime

Artificial Intelligence has also become a significant tool in cyber-enabled financial crime. Criminal organisations increasingly employ AI to generate phishing emails, clone voices, impersonate business executives and automate fraudulent communications.[57]

Voice-cloning technologies, in particular, have enabled fraudsters to imitate family members or senior corporate officials with remarkable accuracy, persuading victims to transfer substantial sums of money. Such offences continue to be prosecuted under existing criminal laws governing cheating, extortion, and cyber fraud under the BNS, 2023, and Section 66D of the IT Act, 2000.[58]

However, these incidents also demonstrate the broader regulatory challenge. AI frequently operates as an instrument facilitating criminal conduct rather than acting as an independent offender. Consequently, legal responsibility must continue to rest primarily upon human actors while simultaneously recognising the enhanced risks created by increasingly sophisticated AI technologies.

7.7 Analysis

The foregoing examples demonstrate a recurring pattern. In each instance, Artificial Intelligence contributes to harmful consequences, yet responsibility cannot easily be attributed to a single participant.

Traditional criminal law assumes a relatively direct relationship between offender, conduct and consequence. AI disrupts this relationship by introducing multiple actors into the decision-making process, including developers, deployers, users, platform operators and organisations responsible for governance. Existing doctrines remain capable of addressing certain forms of misconduct but often struggle where autonomous learning, distributed decision-making and algorithmic adaptation become significant causal factors.

[57] Europol, The Impact of Large Language Models on Law Enforcement (2023).
[58] BNS, 2023, and Section 66D of the IT Act, 2000.

These practical examples therefore reinforce the central argument advanced in the preceding chapter: the principal challenge lies not in recognising AI as a legal offender, but in constructing an effective framework for allocating responsibility among the human actors who create, deploy and supervise AI systems.

While existing legal principles continue to provide partial solutions, they were not designed for technologies capable of learning, adapting and generating independent outputs. Consequently, India must move beyond fragmented regulation towards a comprehensive legal framework capable of balancing innovation with accountability.

8. Towards a Regulatory Framework for Artificial Intelligence in India

The preceding chapters have demonstrated that although India has taken significant steps towards promoting Artificial Intelligence through policy initiatives and existing legislation, the present regulatory framework remains fragmented. The Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and various executive guidelines regulate isolated aspects of AI without establishing a comprehensive legal framework governing its development, deployment, and accountability.[59]

As AI systems continue to influence healthcare, criminal justice, finance, education, governance, and transportation, reliance upon indirect regulation is likely to create increasing legal uncertainty. The challenge before India is therefore not whether AI should be regulated, but how it should be regulated in a manner that simultaneously protects innovation, individual rights, and public safety.

This chapter proposes a principled regulatory framework that seeks to balance technological advancement with legal accountability.

8.1 Guiding Principles for AI Regulation

Any future legislation governing Artificial Intelligence in India should be founded upon certain core legal principles rather than attempting to regulate every technological development individually.

[59] Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, Report of the AI Governance Guidelines Development Committee (2025).

The first principle is *accountability*. Every AI system should have an identifiable person or organisation legally responsible for its deployment and operation. The absence of clear accountability may result in victims being left without an effective legal remedy.[60]

The second principle is *transparency*. Individuals affected by significant AI-assisted decisions should be informed whenever such decisions are made using automated systems. Where feasible, developers should maintain sufficient documentation explaining how AI systems reach particular conclusions.[61]

Thirdly, AI regulation must preserve *meaningful human oversight*. Decisions affecting life, liberty, healthcare, employment, criminal justice, or other fundamental rights should never be left entirely to autonomous systems without the possibility of human review.[62]

Another essential principle is *fairness and non-discrimination*. AI systems should be regularly evaluated to minimise algorithmic bias capable of producing discriminatory outcomes on the basis of race, gender, religion, disability, caste, or other protected characteristics.[63]

Finally, regulation should remain *technology-neutral*. Rather than regulating specific software, legislation should regulate the risks created by AI applications. Such an approach allows the law to remain relevant despite rapid technological change.

8.2 Risk-Based Classification of Artificial Intelligence

India may benefit from adopting a risk-based regulatory model similar to that employed by the European Union, while adapting it to domestic legal and socio-economic conditions.[64]

Low-risk AI systems, such as recommendation engines, spam filters, grammar correction software, and customer service chatbots, should remain subject to minimal regulatory obligations. Excessive regulation of such technologies may unnecessarily discourage innovation.

[60] OECD, Recommendation of the Council on Artificial Intelligence (2019), Principle 1.3 (Accountability).
[61] Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts. 13–15 (Transparency and Human Oversight).
[62] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021), Principles of Human Oversight and Determination.
[63] NITI Aayog, Responsible AI for All: Operationalizing Principles for Responsible AI (2021).
[64] Regulation (EU) 2024/1689, arts. 5–7 (Risk Classification of AI Systems).

Medium-risk AI systems, including AI deployed in recruitment, banking, education, and insurance, should comply with transparency obligations, periodic audits, and mechanisms enabling human review of important decisions.

High-risk AI systems should include technologies deployed in healthcare, criminal justice, policing, critical infrastructure, autonomous transportation, and national security. Such systems should undergo mandatory certification, independent safety audits, impact assessments, and continuous monitoring before deployment.

Finally, certain categories of AI should be prohibited altogether where their risks substantially outweigh any potential public benefit. Examples may include AI designed exclusively for unlawful surveillance, manipulative behavioural exploitation, or autonomous lethal decision-making without meaningful human control.

A risk-based model ensures that regulatory burdens remain proportionate to the degree of potential harm.

8.3 Allocation of Criminal Liability

One of the greatest shortcomings of the present legal framework is the absence of clear principles governing criminal responsibility where AI contributes to harmful consequences.

The traditional approach of identifying a single offender is often inadequate because AI systems operate through the combined actions of developers, deployers, users, and organisations. Consequently, liability should be allocated according to each participant's degree of control over the system.

Developers should incur liability where harm results from negligent design, inadequate testing, deliberate concealment of known defects, or failure to implement reasonable safeguards.

Deployers, including hospitals, corporations, financial institutions, and government agencies, should remain responsible where AI systems are implemented without appropriate supervision or are used beyond their intended purposes.

Users should incur liability where AI is knowingly employed for unlawful purposes, including fraud, identity theft, cybercrime, harassment, production of deepfakes, or dissemination of

unlawful material.

Corporate entities should remain liable where organisational failures contribute substantially to AI-related harm, particularly where inadequate governance, compliance failures, or commercial negligence facilitate unlawful outcomes.

This shared liability model better reflects the distributed nature of AI decision-making while ensuring that responsibility ultimately remains attributable to identifiable human actors.

8.4 Establishment of an Artificial Intelligence Regulatory Authority

India should consider establishing an independent statutory authority responsible for regulating Artificial Intelligence across sectors.

The proposed Artificial Intelligence Regulatory Authority of India (AIRAI) could perform functions including registration of high-risk AI systems, issuance of regulatory standards, certification of AI applications, investigation of AI-related incidents, coordination with sectoral regulators, publication of safety guidelines, and maintenance of a national registry of high-risk AI deployments.

The Authority should also possess powers to impose administrative penalties for non-compliance, require corrective measures, suspend unsafe AI systems, and recommend criminal prosecution where appropriate.

Such an institution would promote regulatory consistency while reducing fragmentation across different sectors.

8.5 Mandatory Algorithmic Audits

High-risk AI systems should undergo periodic independent audits before and after deployment. Algorithmic audits should evaluate data quality, cybersecurity safeguards, bias, transparency, explainability, accuracy, robustness, and compliance with applicable legal standards. Audit reports should be retained for regulatory inspection and made available to competent authorities where required. Incident-reporting obligations should also be introduced. Organisations deploying high-risk AI should be required to notify regulators whenever AI contributes to significant harm, cybersecurity breaches, or substantial failures affecting public

safety. Such mechanisms would encourage continuous monitoring rather than relying solely upon post-incident litigation.

8.6 Strengthening Criminal Law

Existing criminal legislation should be amended to expressly recognise AI-assisted offences without abandoning the principle that criminal liability ultimately belongs to human actors.

Legislation should clearly specify circumstances under which developers, deployers, corporations, and users may incur criminal liability arising from AI-related conduct. The law should distinguish between intentional misuse, negligent deployment, unforeseeable system failures, and criminal exploitation by third parties.

Additionally, sentencing courts should be empowered to consider the extent to which AI contributed to the commission of an offence while determining individual culpability.

Such statutory clarification would significantly reduce uncertainty for courts, investigators, prosecutors, and technology developers.

8.7 International Cooperation

Artificial Intelligence frequently operates across national borders. Training data may originate in one country, software may be developed in another, cloud infrastructure may be located elsewhere, and harmful consequences may occur within India.

Accordingly, domestic legislation alone cannot fully regulate AI. India should actively participate in international initiatives concerning AI governance, cybersecurity, cross-border investigations, technical standards, and information sharing. Harmonisation with globally accepted principles would facilitate international cooperation while reducing regulatory inconsistency.

A future regulatory framework should therefore move beyond reactive governance and adopt a comprehensive model based upon accountability, transparency, human oversight, proportional regulation, and shared responsibility. Such a framework would not only strengthen public confidence in Artificial Intelligence but would also provide greater certainty for innovators, regulators, and courts. Ultimately, the objective of regulation to ensure that

technological advancement remains consistent with constitutional values, the rule of law, and the protection of human dignity.

9. Findings and Recommendations

9.1 Major Findings of the Study

The present study demonstrates that Artificial Intelligence has evolved from a technological innovation into a transformative force capable of influencing almost every aspect of human life. Unlike conventional software, AI systems possess the ability to analyse large volumes of data, learn from experience, adapt to changing circumstances, and generate outputs with varying degrees of autonomy. These characteristics have challenged several traditional assumptions upon which modern legal systems have historically operated.

One of the principal findings of this research is that the existing Indian legal framework does not comprehensively regulate Artificial Intelligence. Although statutes such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 regulate specific aspects of digital technology and personal data, neither statute was enacted with autonomous AI systems in mind. Consequently, issues relating to algorithmic accountability, explainability, criminal responsibility, autonomous decision-making and allocation of liability remain largely unresolved.[65]

The study further establishes that traditional principles of criminal liability are inherently human-centric. The doctrines of *actus reus* and *mens rea* presuppose the existence of a human actor capable of intention, knowledge or negligence. Artificial Intelligence, despite its increasingly sophisticated capabilities, lacks legal personality, consciousness and moral agency. As a result, the direct attribution of criminal liability to AI is presently incompatible with existing legal doctrine.

Another significant finding emerging from the comparative analysis is that jurisdictions across the world have adopted different regulatory philosophies. The European Union has implemented a comprehensive risk-based legislative framework through the Artificial Intelligence Act, whereas the United States continues to rely primarily upon sector-specific

[65] Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, Report of the AI Governance Guidelines Development Committee (2025).

regulation supplemented by executive guidance and voluntary standards. China has adopted a comparatively interventionist model characterised by extensive governmental oversight. India's approach remains fragmented and policy-driven, reflecting a preference for encouraging innovation while postponing comprehensive legislative intervention.[66]

The study also finds that no single traditional doctrine, including vicarious liability, corporate criminal liability or strict liability, is independently capable of resolving every instance of AI-related harm. Autonomous AI systems frequently involve multiple participants, including developers, deployers, users, cloud service providers and corporate entities. Responsibility is therefore often distributed rather than concentrated in one identifiable actor.

Finally, this research establishes that regulation should be viewed as an an effective regulatory framework promotes innovation by creating legal certainty, protecting public confidence and encouraging responsible technological advancement.

9.2 Recommendations

(A) Enact a Comprehensive Artificial Intelligence Legislation

India should enact dedicated legislation governing Artificial Intelligence instead of relying exclusively upon indirect regulation through existing statutes. A comprehensive AI statute would provide legal certainty regarding definitions, accountability, liability standards, compliance obligations and enforcement mechanisms while ensuring consistency across sectors.

(B) Introduce a Risk-Based Regulatory Model

Legislation should classify AI systems according to the degree of risk they present. Low-risk systems should remain subject to minimal compliance obligations, whereas high-risk applications deployed in healthcare, criminal justice, transportation, finance and critical infrastructure should undergo mandatory certification, periodic audits and enhanced regulatory supervision. Such an approach would promote proportional regulation without unnecessarily

[66] Regulation (EU) 2024/1689 (Artificial Intelligence Act); National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0) (2023); Interim Measures for the Management of Generative Artificial Intelligence Services (China, 2023).

restricting innovation.[67]

(C) Clearly Define Criminal Liability

The legislature should expressly clarify the circumstances under which criminal liability may arise in relation to AI-assisted harm. Liability should be allocated according to the degree of control exercised by various stakeholders, including developers, deployers, users and corporate entities. Such statutory clarification would reduce uncertainty for investigators, prosecutors and courts.

(D) Establish an Independent Artificial Intelligence Regulatory Authority

A specialised statutory authority should be constituted to regulate high-risk AI systems, formulate technical standards, conduct investigations, certify AI applications and coordinate with sectoral regulators. Such an institution would ensure consistency in AI governance while facilitating effective enforcement.

(E) Mandate Transparency and Explainability

Developers of high-risk AI systems should maintain adequate documentation explaining system architecture, training methodologies, testing procedures and decision-making processes. Individuals significantly affected by AI-assisted decisions should have access to meaningful explanations wherever practicable. Transparency strengthens public confidence and facilitates legal accountability.

(F) Introduce Mandatory Algorithmic Audits

Independent algorithmic audits should be conducted before and after deployment of high-risk AI systems. These audits should evaluate bias, cybersecurity, robustness, explainability, accuracy and compliance with applicable legal standards. Organisations should also be required to report significant AI-related incidents to the competent regulatory authority within a prescribed time period.

[67] Regulation (EU) 2024/1689, arts. 5–7 (risk classification of AI systems).

(G) Strengthen Data Governance

The Digital Personal Data Protection Act, 2023 should be supplemented with specific provisions governing AI-driven profiling, automated decision-making and algorithmic fairness. Data protection alone cannot adequately regulate Artificial Intelligence unless accompanied by broader obligations relating to accountability and transparency.

(H) Promote Ethical AI Development

Ethical principles should form an integral component of India's AI governance framework. Public and private organisations should adopt policies ensuring fairness, non-discrimination, privacy, human oversight and responsible innovation throughout the AI lifecycle. Ethical governance reduces legal risks while promoting socially beneficial technological development.

(I) Enhance Judicial and Investigative Capacity

The successful regulation of Artificial Intelligence requires institutional preparedness. Judges, prosecutors, investigating agencies and regulatory authorities should receive specialised training regarding AI technologies, digital evidence, algorithmic decision-making and emerging cyber-enabled offences. Improved institutional capacity will enable more effective adjudication of AI-related disputes.

(J) Encourage International Cooperation

Given the transnational nature of Artificial Intelligence, India should continue participating in international initiatives relating to AI governance, cybersecurity, technical standards and cross-border enforcement. Harmonisation with internationally recognised principles will facilitate cooperation while preserving India's constitutional and developmental priorities.

10. Conclusion

Artificial Intelligence has rapidly evolved from a technological innovation into an indispensable component of modern society. Its integration into healthcare, finance, transportation, governance, education, law enforcement, and the legal profession demonstrates that AI is no longer a futuristic concept but an everyday reality. While these developments have generated unprecedented opportunities for economic growth, efficiency, and innovation, they

have simultaneously exposed significant shortcomings within existing legal frameworks. The law, which has historically evolved in response to technological advancement, now faces one of its most complex challenges: regulating systems capable of learning, adapting, and making decisions with varying degrees of autonomy.

The primary objective of this study was to examine whether the existing legal framework in India is adequate to regulate Artificial Intelligence and address the issue of legal liability arising from its use. The research demonstrates that although India has adopted several important legislative and policy measures, including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the National Strategy for Artificial Intelligence, and the AI Governance Guidelines, these measures regulate only isolated aspects of Artificial Intelligence rather than the technology as a whole. The present framework remains fragmented, leaving substantial uncertainty regarding accountability, explainability, criminal liability, and governance of autonomous AI systems.[68]

The study further establishes that the application of traditional criminal law principles to Artificial Intelligence presents significant doctrinal difficulties. Concepts such as *actus reus* and *mens rea* were developed on the assumption that criminal conduct originates from human actors capable of intention, knowledge, recklessness, or negligence. Artificial Intelligence lacks legal personality, consciousness, and moral agency. Consequently, AI cannot presently be regarded as an independent bearer of criminal responsibility under Indian law. This does not, however, diminish the need for accountability. Instead, it requires the law to develop clearer principles for allocating responsibility among the human actors involved in the design, deployment, supervision, and use of AI systems.

The comparative analysis undertaken in this paper demonstrates that jurisdictions across the world have adopted differing approaches to AI governance. The European Union has implemented a comprehensive risk-based legislative framework through the Artificial Intelligence Act, while the United States continues to rely largely upon sector-specific regulation supplemented by executive guidance and technical standards. China has adopted a comparatively interventionist model characterised by extensive governmental oversight. Although these approaches differ considerably, they reveal a common recognition that AI

[68] Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, Report of the AI Governance Guidelines Development Committee (2025); NITI Aayog, National Strategy for Artificial Intelligence (2018).

cannot remain entirely outside legal regulation. India, therefore, has the opportunity to learn from international experience while developing a framework that reflects its own constitutional values, institutional capacity, and developmental priorities.

This research also highlights that AI-related harm rarely results from the conduct of a single participant. Rather, modern AI systems function through an interconnected network involving developers, deployers, users, corporations, cloud service providers, and regulators. Attempting to identify one individual as solely responsible may therefore oversimplify the realities of autonomous decision-making. A more effective legal response lies in recognising that responsibility may be distributed according to the degree of control exercised by each participant. Such an approach preserves the foundational principles of criminal law while acknowledging the practical realities of emerging technologies.

Another important finding of this study is that regulation should not be viewed as an obstacle to innovation. Throughout history, law has served not only to prohibit harmful conduct but also to create certainty, facilitate commerce, and strengthen public confidence in new technologies. Artificial Intelligence should be viewed no differently. A well-designed regulatory framework promotes responsible innovation by providing clear legal standards, protecting individual rights, and encouraging public trust in AI-enabled systems. Conversely, regulatory uncertainty may undermine both technological development and public confidence.

Accordingly, this paper proposes that India adopt a comprehensive regulatory framework founded upon the principles of accountability, transparency, fairness, explainability, human oversight, and risk-based regulation. AI regulation should distinguish between systems according to the degree of risk they present. High-risk AI systems deployed in healthcare, criminal justice, transportation, and public administration should be subject to enhanced oversight, independent audits, and clearly defined liability standards. At the same time, low-risk applications should remain sufficiently flexible to encourage continued research and innovation.

The rapid evolution of Artificial Intelligence also demonstrates that legislation alone cannot provide every answer. Effective AI governance will require continuous collaboration between legislators, courts, regulatory authorities, technology developers, industry stakeholders, and civil society. Judicial interpretation will play an increasingly significant role in adapting established legal principles to novel factual circumstances, particularly where existing statutes

remain silent. The evolution of AI regulation must therefore be viewed as an ongoing legal process rather than a single legislative event.

In conclusion, Artificial Intelligence represents one of the defining legal challenges of the twenty-first century. The question is no longer whether AI should be regulated, but whether existing legal systems are capable of evolving quickly enough to regulate technologies that continue to advance at an extraordinary pace. India possesses both the opportunity and the responsibility to develop a balanced legal framework that protects innovation while safeguarding constitutional values, individual rights, and public safety. Such a framework should not seek to impede technological progress but rather to ensure that progress remains firmly anchored in the principles of justice, accountability, and the rule of law.

Ultimately, the future of Artificial Intelligence will be shaped by the ability of legal systems to ensure that innovation serves humanity without compromising the values upon which democratic societies are founded.