



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]



Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

“Law in the Age of Artificial Intelligence: A Fundamental Perspective”

Organised by KES’ Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: <https://doi.org/10.70183/lijdlr.2026.v4si1.14>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE

About the College



KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

KANDIVLI EDUCATION SOCIETY

Established 1936



Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

EDUCATIONAL COMMITMENT

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

LAW IN THE AGE OF ARTIFICIAL INTELLIGENCE

A Fundamental Perspective



ABOUT THE INTERNATIONAL CONFERENCE

The International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective” provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

PRINCIPAL'S MESSAGE

KES' Shri. Jayantilal H. Patel Law College



It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective.”

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

DR. VIRAL DAVE

I/c. Principal

KES' Shri. Jayantilal H. Patel Law College

ORGANISING COMMITTEE

International Conference on Law in the Age of Artificial Intelligence



I/c. Principal

Dr. Viral Dave

Convenor

Mr. Mahavir Mandot

Co-Convenors

Dr. Shweta Vijendra Pathak

Ms. Priyanka Khakhadia

Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

*Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of
Doctrinal Legal Research [Volume IV, Special Issue I, 2026]*

AI AND LIABILITY IN LEGAL SYSTEMS

Jinal Suresh Thakur¹

I. ABSTRACT

Artificial Intelligence (AI) is transforming the functioning of legal systems by assisting in legal research, document review, predictive analysis, administrative decision-making, and other professional tasks. While these technologies improve efficiency, reduce costs, and support faster decision-making, they also raise complex questions of legal accountability when an AI system causes harm. This paper examines the central issue of liability for AI-related harm under Indian law, particularly whether responsibility should rest with developers, manufacturers, deployers, users, or, in limited theoretical discussions, the AI system itself. It analyses the application and limitations of existing legal principles, including criminal liability, civil liability, negligence, product liability, absolute liability, and vicarious liability. The paper also evaluates whether artificial intelligence can be recognised as a legal person under Indian law and explains why the absence of intent, conscience, and moral judgment makes such recognition difficult within the current legal framework. The study adopts a doctrinal and comparative approach by examining Indian statutes, case law, scholarly writings, and international developments, particularly the European Union Artificial Intelligence Act, 2024. It argues that existing Indian laws, including the Information Technology Act, 2000 and the Consumer Protection Act, 2019, were primarily designed for human conduct and conventional products, and therefore do not adequately address autonomous or algorithmic decision-making. The paper recommends that India enact a dedicated AI liability framework, amend consumer protection law to cover AI-enabled goods and services, introduce certification and oversight mechanisms for high-risk AI systems, and develop compensation models for serious AI-caused harm. Such reforms are necessary to protect victims, ensure accountability, and promote responsible innovation.

¹ 3rd Semester, LL.M (Business Law), Student at KES' Shri Jayantilal H. Patel Law College, Mumbai (India).Email:thakurjinal@gmail.com

II. KEYWORDS

Artificial Intelligence; Liability; Legal Personhood; Product Liability; India.

III. INTRODUCTION

In the field of law, Artificial Intelligence is growing rapidly and is becoming an important part of the legal profession, raising many new and serious questions about how the law should respond. One of the most important issues that has come up is who should be held responsible when an AI system causes harm? Today, AI is being used in courts, hospitals, banks, and many other places. In India, tools like Nyaay AI and Adalat AI are already helping in the judicial system.

But when these AI systems make mistakes and cause harm to someone, Indian law does not give a clear answer about who should be held responsible. This is the main problem this paper is trying to solve. The framework of legal profession before the AI system came into reality and the current system with the AI has drastically changed the working pattern of law. The current approach to AI liability relies on fault and causation, but in India it remains unclear who should be held responsible for decisions made by AI systems.

This issue is especially important in India because Indian laws like the IT Act, 2000 and the Consumer Protection Act, 2019 were made for human actions, not for AI systems. India does not yet have a dedicated statute that comprehensively determines liability for harm caused by artificial intelligence systems. However, it is no longer accurate to say that no institutional steps have been taken. In November 2025, MeitY released the India AI Governance Guidelines under the IndiaAI Mission, adopting a light-touch governance approach and recognising the relevance of existing laws such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Consumer Protection Act, 2019 to AI-related risks.

Nevertheless, these measures do not yet provide a specific statutory liability framework for autonomous AI-caused harm, and this continuing gap requires

clearer legislative attention. The moral dimension of attributing liability to AI systems remains a heavily contested issue in contemporary legal discourse. There are two sides for this debating over that, it is not prejudicial to hold AI accountable, as a result of the fact that AI is not fully capable to comprehend their action's consequence. And on the other hand, AI system has to be hold accountable/ liable to prevent destructive behaviour and ensure that fatalities of AI - regarding harm are expiated.

The Indian government has now taken material policy and institutional steps toward AI governance, particularly through the India AI Governance Guidelines released by MeitY in November 2025 and the RBI's FREE-AI Committee report submitted in August 2025 for the financial sector. However, these developments remain primarily governance-oriented and sectoral in nature. They do not, by themselves, create a dedicated statutory liability regime identifying responsibility among developers, manufacturers, deployers, and users when AI systems cause harm.

This paper is divided into several parts. First, it looks at the research problem and analyses different types of liability such as criminal liability, civil liability, product liability, absolute liability, and vicarious liability under Indian law. It also compares India's position with international frameworks like the EU AI Act, 2024. Then it examines whether AI can be given legal personhood under Indian law. Finally, the paper concludes with suggestions on how India should create a new and dedicated law to deal with AI liability. There is an urgent need and necessity to develop the legal framework which is transparent, effective, and morally ethical.

A. Research Hypothesis

1. Current legal frameworks such as tort and product liability Laws, strict liability under Indian law are insufficient, on their own, to address harm caused by autonomous artificial intelligence systems. these laws would need to be adapted through judicial interpretation or legislative

reform to provide effective remedies and accountability for AI-related harm.

2. The lack of a specific statutory framework on artificial intelligence liability in India leads to uncertainty and inconsistent attribution of responsibility among developers, manufacturer, and users of AI systems.
3. In cases where autonomous AI systems make decisions, strict liability and no - fault liability is more effective than negligence - based liability because they allow victims to receive compensation more quickly and easily for AI-related harm.

B. Research Objectives

1. To examine liability in cases of harm caused by AI systems, focusing on whether the developer, user, or manufacturer can be held responsible.
2. To explore legal remedies available to victims and assess the adequacy of statutory provisions under Indian law.
3. To investigate if AI systems can be considered legal persons under Indian law, and what this means for liability.
4. To evaluate the current legal frameworks and their effectiveness in addressing harm caused by AI systems.
5. To compare the AI liability framework under the European Union AI Act, 2024, and the symbolic recognition of AI legal status in Saudi Arabia, and to assess how these international developments might inform and influence the creation of a dedicated AI liability framework in India.

C. Research Questions

1. Who should bear legal liability when an autonomous artificial intelligence system causes harm under the existing Indian legal framework?

2. Are the present principles of tort law, product liability, strict liability, and vicarious liability sufficient to address harm caused by AI systems in India?
3. Can artificial intelligence systems be granted legal personhood under Indian law, and what would be the implications of such recognition for civil and criminal liability?
4. What remedies are available to victims of AI-related harm under existing Indian statutes, including the Consumer Protection Act, 2019 and the Information Technology Act, 2000?
5. How can international regulatory developments, particularly the European Union AI Act, 2024, guide India in developing a dedicated legal framework for AI liability?

D. Research Methodology

This study adopts a doctrinal and analytical legal research methodology. It is based primarily on the examination of statutory provisions, judicial decisions, and established principles of Indian law relating to tort liability, product liability, strict liability, vicarious liability, and legal personhood. The study also relies on secondary sources, including journal articles, books, reports, and scholarly commentaries, to analyse the legal challenges arising from harm caused by artificial intelligence systems.

The research further follows a comparative approach by examining international developments, particularly the European Union Artificial Intelligence Act, 2024, and considering their relevance for the Indian legal framework. This methodology is used to identify gaps in existing Indian law and to suggest the need for a dedicated and accountable legal framework governing AI-related liability.

E. Scope Of the Study

This study majorly focuses on whom the liability rests in case of harm caused by the artificial intelligence (AI), with a specific focus on India's legal framework.

The paper analyses whether current laws in India — like Tort Law, Strict Liability and Product Liability under the Consumer Protection Act, 2019 — can be applied to situations where AI causes harm. It also examines fairness and the accessibility of legal remedies for people who are affected by AI decisions. Instead, it uses legal research methods — such as analysing statutes, court judgements, and research work to identify gaps and challenges in applying existing laws to AI. The aim is to offer suggestions for how India's legal system might evolve to better address liability issues related to AI.

IV. RESEARCH & ANALYSIS

The rapid growth of the AI in every field and sector has become part of each and every individual lives. Although, the administrative department has worked upon to build and/or slowly filling the loopholes of technical shortcomings, inferiority existing in the legal system of India. The instance for the growth by the government in this direction is seen from establishment of e-court projects (National Judicial Digital Transformation), to now, AI-enabled tools in courts (Nyaay AI and Adalat AI), are the major changes towards the development in AI navigated legal justice system.

Liability in legal system covered under several types. Indian laws were largely designed around human conduct, corporate responsibility, conventional products, and identifiable intermediaries rather than autonomous AI systems. The India AI Governance Guidelines, 2025 attempt to address this uncertainty by mapping AI-related risks to existing legal frameworks and by proposing institutional mechanisms such as an AI Governance Group, a Technology & Policy Expert Committee, and an AI Safety Institute. However, because the Guidelines follow a non-legislative and light-touch model, uncertainty remains regarding the precise attribution of civil, criminal, product, and vicarious liability when autonomous AI systems cause harm.

The primary law regulating digital activities, including data protection and cybersecurity concerns relevant to AI applications, is the Information Technology Act, 2000. Alongside it, the Digital Personal Data Protection Act, 2023 plays an

important role in shaping the use of artificial intelligence by prescribing obligations relating to the collection, use, storage, and protection of digital personal data, with emphasis on consent, privacy, and lawful processing.

This framework has been further operationalised through the Digital Personal Data Protection Rules, 2025, notified in November 2025. The Rules provide the practical compliance architecture for the Act, including requirements relating to consent mechanisms, personal data breach notification, grievance redressal, and the functioning of the Data Protection Board of India as a digital regulatory body. They also introduce a phased implementation timeline, giving data fiduciaries time to comply with different obligations, with several core compliance requirements becoming applicable by May 2027.

These Rules are particularly relevant for AI developers and deployers because AI systems often depend on large volumes of personal data for training, testing, deployment, profiling, or automated decision-making. Where such entities determine the purpose and mean of processing personal data, they may qualify as data fiduciaries and must ensure lawful consent, data security safeguards, breach reporting, and compliance with directions of the Data Protection Board. Therefore, while the DPDP framework does not directly create a complete AI liability regime, it significantly affects AI-related accountability where harm arises from unlawful, unsafe, or non-consensual use of personal data.

A. Criminal Liability

Criminal liability for AI-related harm in India must now be examined with reference to the Bharatiya Nyaya Sanhita, 2023 (BNS), which has replaced the Indian Penal Code for substantive criminal offences, and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), which governs criminal procedure. Although Gabriel Hallevy's theory explains that AI systems may appear to perform an act or omission resembling *actus reus*, and that some offences may involve *mens rea* while others operate on negligence or strict-liability standards, Indian criminal law still attributes liability to legally recognised persons rather than to AI systems themselves. Therefore, where an AI system causes harm, the inquiry under the

BNS should focus on whether a developer, deployer, manufacturer, operator, or user acted with intention, knowledge, rashness, negligence, or unlawful omission.

Hallevy proposes a three-part approach to investigate AI system crimes:

1. AI liability when another is responsible for the crime:

A minor, someone with an intellectual disability, or a creature who commits a crime but lacks the mental capacity to form mens rea under criminal culpability are examples of innocent agents. The same remains true in the case of serious responsibility. However, the person who gives the instruction will be held liable if they are used as a tool by a criminal to carry out their activities which are legally not sustainable, justifiable, tenable. Because of this, the AI system is viewed as an innocent actor in this idea, however the person giving it instructions is seen as a criminal.

2. The liability of AI's natural likely outcome:

Under Indian law, the “natural probable consequence” model is better understood as a basis for assessing the conduct of the human actor connected with the AI system. If a reasonable developer, deployer, or user could foresee that an AI system might cause harm because of unsafe design, inadequate testing, defective training data, absence of human oversight, or reckless deployment, criminal responsibility may arise under BNS provisions dealing with rash or negligent conduct. For example, where AI-caused harm results in death, Section 106 of the BNS on causing death by negligence may become relevant, provided the prosecution can establish the required causal connection between the accused person’s rash or negligent act and the resulting death.

For instance, if a robot-assisted surgical system performs an unintended movement contrary to the surgeon’s commands during a procedure in an Indian hospital, liability cannot automatically be shifted to the AI system as an independent criminal actor. The relevant inquiry would be whether the surgeon, hospital, manufacturer, programmer, or maintenance provider failed to exercise

the degree of care required in the circumstances. If death or bodily injury results from grossly unsafe deployment, defective maintenance, inadequate supervision, or negligent programming, the matter may be analysed under the BNS provisions governing rash or negligent acts, including Section 106 where death is caused by negligence. The BNSS would then govern investigation, prosecution, evidence collection, and trial procedure.

AI systems cannot be recognized as legal persons and so cannot be held criminally or civilly liable. However, when an offence occurs due to careless use, fails to supervise it, or deliberate misuse of an AI system by a human, the responsibility cannot be transferred to the AI itself. In such instances, culpability must fall on the user whose carelessness caused or contributed to the offense.

In the case of Kenji Urada, 37 years old worker, at the Akashi plant of Kawasaki Heavy Industries, a robot was being used for specific manufacturing tasks. While Kenji was carrying out repair work on the machine, he failed to switch it off. As a result, the robot mistook him for an obstruction and forcefully pushed him into a nearby machine with its hydraulic arm. The impact was fatal, and Kenji died almost immediately.

3. The Direct Liability of AI:

In strict-liability or regulatory offences, the prosecution may not always be required to prove intention in the same manner as serious mens rea-based offences. However, even in such cases, Indian law does not presently recognise AI software as a criminal person. In the example of an autonomous vehicle exceeding the speed limit or causing an accident, liability would therefore have to be mapped onto the conduct of legally recognised persons, such as the vehicle owner, operator, deployer, manufacturer, or software provider, depending on the statutory duty breached.

Where rash driving or negligent operation causes injury or death, the relevant BNS provisions, including those concerning rash driving and causing death by negligence, should be considered along with applicable motor vehicle and

regulatory laws. Thus, Hallevy's direct-liability model may be useful theoretically, but under the current BNS framework it requires adaptation so that criminal responsibility is attributed to human or corporate actors connected with the AI system rather than to the AI itself.

B. Civil Liability

When a software defect causes harm, it is generally treated as negligence rather than a criminal offence. To establish negligence, three elements are considered: the defendant owed a duty of care, that duty was breached, and the plaintiff suffered harm as a result of the breach

According to Gerstner, there are several ways an AI system could fail in its duty of care, including:

1. The developer not identifying errors in the programming,
2. Having an inadequate or incomplete knowledge base,
3. Mistakes caused by incorrect user input or over-reliance on the AI system.

C. Product Liability

AI systems, like other products, can be covered under product liability laws. If an Artificial Intelligence system causes harm, the maker or developer could be held responsible for faults in the product's design, how it was made or failure to provide proper warnings. In India, the Consumer Protection Act, 2019, Provides a framework for product responsibility, notably in the context of consumer goods. While the Act does not expressly mention artificial intelligence, it might be amended to include liability for defective AI systems or services delivered to consumers.

V. LEGAL PERSONHOOD AND STATUS OF AI

In Indian law, legal status is granted not only to humans but also to companies and corporations. However, such status has not been extended to technology, such as robots. In Saudi Arabia, a robot named Sophia was granted symbolic

citizenship in 2017, which included certain rights and duties. This gesture, however, was largely symbolic and has been widely criticized by legal scholars. It is often viewed as a publicity-driven move rather than a legally enforceable grant of rights comparable to human or corporate personhood. A person can make their own decisions because they are independent, but AI is created by humans and only acts according to the instructions programmed into it.

Companies depend upon identifiable human agents such as directors, officers, and employees to make decisions that can be examined and attributed for liability purposes, whereas AI systems use algorithmic processes that do not involve intent, conscience, or moral judgment, making it much harder to apply traditional legal concepts like fault, intent, or mens rea.

Another key distinction between AI and corporations is that, while companies are self-regulating, and are held accountable by consumers and shareholders, AI lacks legal personality and is thus not subject to the law.

VI. ANALYSIS

Some experts suggest that AI could be liable for autonomous actions, Indian law currently holds humans responsible because, the Indian law still considers that AI doesn't have legal status. They have no liability and responsibility in legal system. That AI systems still lacks of consideration, moral grounds and human application of mind which results in limitation to the liability of AI. As human beings holds unique potential of containing knowledge which is effective in all the activities performed by an individual.

On the other hand, AI does not contain legal personality which makes AI system not liable for the action produced by the work of the AI, if any criminal nature liability arises, mens rea is necessary component to prove the same. It appears hypothetical that AI systems will break laws that require knowledge of criminal act being committed. However, they might still break laws where a 'reasonable person' would foresee that their actions could cause an offence, and they are highly likely to commit strict liability offences. This raises the question of who

should be held accountable: the human giving the instructions or the AI systems. The position in India has evolved.

The government has taken concrete governance steps through the India AI Governance Guidelines, 2025, which recommend a coordinated institutional framework for responsible AI, and through sector-specific initiatives such as the RBI's FREE-AI Committee report for the financial sector. Yet, these measures do not fully resolve the liability problem. They primarily rely on existing statutes and regulatory coordination, whereas autonomous AI harms may require clearer rules on fault, causation, risk classification, compensation, audit obligations, and responsibility among developers, deployers, manufacturers, and users. Therefore, India should build upon these governance initiatives and move toward a fair, ethical, and enforceable AI liability framework.

A. EU AI Act, 2024

The EU Artificial Intelligence Act (Regulation 2024) is the European Union's first comprehensive law aimed at regulating artificial intelligence. This framework sets out unified rules for how AI systems are developed, marketed, and used within the EU. The goal is to ensure that AI technologies are safe, comply with fundamental rights, and align with the core values of the European Union. By creating clear guidelines for AI, the Act seeks to promote innovation while minimizing risks related to safety, privacy, and ethical concerns. It also emphasizes the need for transparency and accountability in the deployment of AI, ensuring that AI systems do not harm individuals or society.

The EU Artificial Intelligence Act holds various parties such as providers, deployers, importers, and distributors responsible for ensuring their AI systems meet regulatory standards. They must set up internal controls, keep proper records, and confirm that the AI systems are fully compliant before they are released to the market. The EU Artificial Intelligence Act (Regulation (EU) 2024) takes a risk-based approach to regulating AI, classifying AI systems into four distinct categories depending on the level of risk they pose to fundamental rights, health, safety, and society.

The compliance requirements differ for each category high-risk systems face stricter regulations, while low-risk systems are subject to fewer requirements or even exemptions. It's crucial for both AI providers (those who develop AI) and deployers (those who use AI) to understand these categories in order to ensure they meet the necessary regulatory standards.

B. NITI Aayog's Responsible AI for All

NITI Aayog has an important policy and advisory role in the AI legal and governance system in India, but it is not a court or legal authority. Instead, it helps design AI policies, ethical principles, and regulatory frameworks for the government. In 2018, NITI Aayog launched a national plan to guide how Artificial Intelligence should be used in India. The key idea behind this plan was "AI for All," which means AI should create value for the entire population, not just a small section.

The strategy aimed to apply AI in important sectors like healthcare, farming, education, urban development, and transport to improve overall efficiency and solve practical problems. At the same time, it stressed the importance of using AI responsibly, often referred to as Responsible AI (RAI), so that systems remain fair, transparent, and safe. As AI adoption increases globally, there is a rising demand for proper rules to control its risks.

To understand these challenges, facial recognition technology was considered as an example. Although this technology can make processes quicker and more effective, it also brings concerns. It may interfere with personal privacy, lead to unfair outcomes, and restrict basic freedoms if not properly managed. In short, the goal is to promote the use of AI for development while ensuring that ethical standards and individual rights are not compromised.

C. Absolute Liability

AI systems, particularly autonomous ones, possess an inherent risk of harm due to their independent functioning. Just as chemical industries or explosive plants were held absolutely liable for accidents in the M.C. Mehta case, AI systems that

perform high-risk tasks (e.g., transportation, healthcare, industrial applications) should similarly bear responsibility for any damage they cause. These systems can make decisions based on algorithms and data, and their failure to act as expected may lead to harm that is not directly preventable by human intervention.

D. Vicarious Liability Principles

In Vicarious liability one person will be responsible for the actions of another. In the case of AI, the developer-user relationship raises questions about accountability:

1. **Developer Liability:** Developers are responsible for ensuring that their AI systems are safe, effective, and transparent. If a harm is caused by an AI system due to a design flaw, developers could be held vicariously liable for the consequences, much like an employer is responsible for the actions of its employees.
2. **User Liability:** Users who deploy AI systems (e.g., autonomous vehicles, AI in healthcare) could also be held liable if they fail to ensure proper oversight or use the systems in ways that lead to harm. For example, a company that uses an AI-driven recruitment tool might be vicariously liable if the system causes discrimination.
3. **Shared Liability:** In cases where both the developer and user are found to be responsible for harm caused by AI, vicarious liability could result in both parties sharing responsibility for damages.

VII. SUGGESTIONS AND RECOMMENDATIONS

1. India should enact a dedicated artificial intelligence liability statute that clearly identifies the duties of developers, manufacturers, deployers, and users. Such a statute should adopt tiered liability standards, applying stricter duties to high-risk AI systems used in sectors such as healthcare, transport, finance, and judicial administration.

2. The Consumer Protection Act, 2019 should be amended to expressly include AI-enabled goods and services within the scope of product liability. This would allow consumers to seek remedies where harm is caused by defective AI design, faulty programming, inadequate warnings, or unsafe deployment of AI-based products and services.
3. A certification and registration framework should be introduced for high-risk AI systems before their commercial or institutional deployment. Developers and deployers should be required to conduct safety audits, maintain transparency records, and ensure human oversight where AI systems may affect life, liberty, privacy, employment, or access to essential services.
4. India should consider creating a compensation fund for serious or catastrophic harm caused by autonomous AI systems. This model may draw from the principle of absolute liability developed in *M.C. Mehta v. Union of India*, so that victims are not denied compensation merely because fault, intent, or causation is difficult to prove in complex AI-related cases.
5. Regulatory authorities should issue sector-specific guidelines for the responsible use of AI, particularly in healthcare, transport, banking, education, policing, and legal services. These guidelines should require fairness, accountability, data protection, explainability, and effective grievance-redressal mechanisms.

VIII. CONCLUSION

In Indian law, AI still does not hold accountability of its own action. Thus, the liability still rests with the human beings due to the absence of legal personality for AI. To reduce uncertainty regarding the attribution of liability, India should move beyond broad governance principles and develop a dedicated legal framework for AI-related harm. The India AI Governance Guidelines, 2025 and the RBI FREE-AI Committee report represent important institutional and sector-specific progress, but they do not conclusively determine liability where

autonomous AI systems cause injury, financial loss, discrimination, or other legally recognised harm.

A dedicated framework should therefore clarify the duties of AI developers, manufacturers, deployers, and users, while preserving innovation through proportionate and risk-based regulation. Individuals who commit crimes utilizing AI systems may be acquitted if sufficient legal measures are not in place, as there is no apparent responsibility. There should also be standards and constraints in place for people who educate AI systems, ensuring that these technologies are designed, deployed, and used with appropriate care.

Lastly, in conclusion, the present legal system in India, although competent for traditional human conduct, is insufficient to hold AI systems and those responsible for their actions accountable. To reduce legal ambiguity and protect victims' rights, the government should build upon the India AI Governance Guidelines, 2025 by enacting specific liability rules for AI-caused harm. Although the present policy approach relies on existing laws and institutional coordination, a dedicated statute or targeted legislative amendments would provide greater certainty on accountability, compensation, due diligence, safety audits, and remedies. Such reform would ensure that India's AI governance model remains not only innovation-friendly but also legally enforceable and victim-centred.

This framework should explicitly clarify the roles and duties of AI developers, manufacturers, and users, holding them accountable if their systems do harm. Furthermore, adequate standards and constraints must be set to guarantee that people who train AI systems exercise due attention and prudence. Until such regulations are enacted, persons who misuse AI risk avoiding accountability, resulting in unfair consequences. By developing a fair, transparent, and effective legal framework, India can ensure that AI's rapid rise benefits society while minimising harm and assuring responsibility.

IX. BIBLIOGRAPHY

A. Statutes, Rules and Regulations

1. The Bharatiya Nyaya Sanhita, 2023.
2. The Bharatiya Nagarik Suraksha Sanhita, 2023.
3. The Consumer Protection Act, 2019.
4. The Digital Personal Data Protection Act, 2023.
5. The Digital Personal Data Protection Rules, 2025.
6. The Information Technology Act, 2000.
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, Official Journal of the European Union, 12 July 2024.

B. Cases

1. *M.C. Mehta v. Union of India*, AIR 1987 SC 1086.
2. *Rylands v. Fletcher*, (1868) LR 3 HL 330.
3. *Donoghue v. Stevenson*, [1932] AC 562.
4. *Salomon v. Salomon & Co. Ltd.*, [1897] AC 22.
5. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
6. *State Bank of India v. Shyama Devi*, (1978) 3 SCC 399.

C. Government Reports, Guidelines and Policy Documents

1. Ministry of Electronics and Information Technology, Government of India, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (2025).
2. Reserve Bank of India, *Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) Committee Report* (August 2025).
3. NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (2018).
4. NITI Aayog, *Responsible AI for All: Approach Document for India, Part 1 – Principles for Responsible AI* (2021).

5. NITI Aayog, *Responsible AI for All: Approach Document for India, Part 2 – Operationalising Principles for Responsible AI* (2021).
6. Ministry of Electronics and Information Technology, Government of India, *National Strategy on Blockchain* (2021).
7. European Commission, *Liability for Artificial Intelligence and Other Emerging Digital Technologies* (Expert Group on Liability and New Technologies, 2019).

D. Books

1. Gabriel Hallevy, *Liability for Crimes Involving Artificial Intelligence Systems* (Springer, 2015).
2. Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson, 2021).
3. Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020).
4. Simon Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law* (Cambridge University Press, 2021).
5. Woodrow Barfield and Ugo Pagallo, eds., *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing, 2018).
6. Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015).

E. Journal Articles and Scholarly Works

1. Gabriel Hallevy, "The Criminal Liability of Artificial Intelligence Entities – From Science Fiction to Legal Social Control" (2010) 4 Akron Intellectual Property Journal 171.
2. Michael E. Gerstner, "Liability Issues with Artificial Intelligence Software" (1993) 33 Santa Clara Law Review 239.
3. Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" (2016) 29 Harvard Journal of Law & Technology 353.

4. Ryan Abbott, "The Reasonable Computer: Disrupting the Paradigm of Tort Liability" (2018) 86 *George Washington Law Review* 1.
5. Mark A. Lemley and Bryan Casey, "Remedies for Robots" (2019) 86 *University of Chicago Law Review* 1311.
6. Mark A. Lemley and Bryan Casey, "You Might Be a Robot" (2019) 105 *Cornell Law Review* 287.
7. Bert-Jaap Koops, Mireille Hildebrandt and David-Olivier Jaquet-Chiffelle, "Bridging the Accountability Gap: Rights for New Entities in the Information Society?" (2010) 11 *Minnesota Journal of Law, Science & Technology* 497.
8. Joanna J. Bryson, Mihailis E. Diamantis and Thomas D. Grant, "Of, For, and By the People: The Legal Lacuna of Synthetic Persons" (2017) 25 *Artificial Intelligence and Law* 273.
9. Yaniv Benhamou and Justine Ferland, "Artificial Intelligence and Damages: Assessing Liability and Calculating Damages" (2020) 12 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 124.
10. Andrea Bertolini, "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules" (2013) 5 *Law, Innovation and Technology* 214.
11. Gerhard Wagner, "Robot Liability" in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer, eds., *Liability for Artificial Intelligence and the Internet of Things* (Nomos, 2019).

F. News and Contemporary References

1. United Press International, "Robot Kills Man" (8 December 1981).
2. Press Information Bureau, Government of India, "MeitY Unveils India AI Governance Guidelines under IndiaAI Mission to Ensure Safe, Inclusive, and Responsible Adoption of Artificial Intelligence across Sectors" (2025).

3. Press Information Bureau, Government of India, “Digital Personal Data Protection Rules, 2025 Notified” (2025).