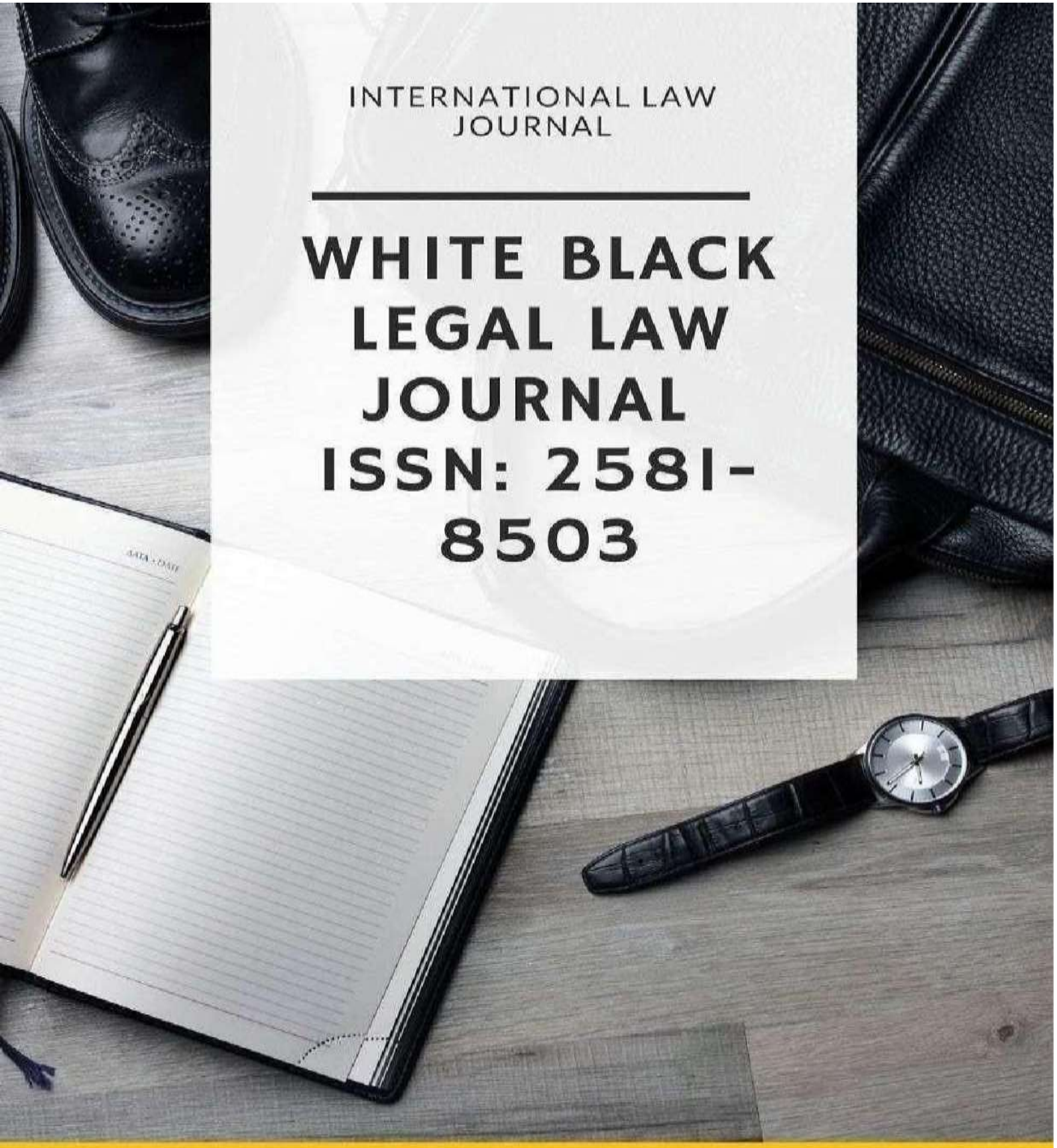

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

GOVERNING THE UNGOVERNED: AIMING TOWARDS A RISK-BASED REGULATORY AND LIABILITY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE IN INDIA

AUTHORED BY - RENU SINGARIA
Research Scholar
Department Of Law, JNV University, Jodhpur (RAJ.)

ABSTRACT

Artificial Intelligence is a present-day technology transforming healthcare, finance, governance, and the justice system. Yet India's legal system, built on statutes that predate the algorithmic age, is profoundly ill-equipped to address the harms AI can cause or to hold responsible parties accountable for those harms.

This paper argues that India faces two linked problems: a lack of a clear liability framework for AI-caused harm and a lack of a dedicated regulatory architecture. The paper compares the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689), the OECD AI Principles, and emerging global norms with Indian laws, including the IT Act 2000, the Digital Personal Data Protection Act 2023, and the Consumer Protection Act 2019. It then identifies structural gaps in India's legal response to the improper usage of AI.

Lastly, the paper proposes a tiered regulatory framework based on risk assessment, the creation of an independent National AI Regulatory Authority, and a shared liability model that distributes responsibility across the AI value chain - from developer to deployer to the state. The paper concludes that in the absence of an urgent and coherent legal intervention, India risks becoming a jurisdiction where the benefits of AI flow to a few while its harms fall upon the many, without legal remedy.

Keywords:
Artificial Intelligence; Liability; Harm; Risk-Based Regulation; Indian Technology Law; Algorithmic Harm; Digital Personal Data Protection Act.

I. INTRODUCTION

There is an old saying that the *'law is always playing catch-up with technology,'* and this is painfully true in the domain of artificial intelligence. Across the world, AI systems are diagnosing disease, creating content, determining creditworthiness, screening job applications, and generating legal documents. In India as well, these transformations are occurring at a rapid pace, almost outstripping the capacity of the Indian legal system to respond. Consequently, there exists a governance and regulatory vacuum: a space where powerful technologies operate, cause harm, and exit, often without a settled liability regime or an institutional authority capable of holding wrongdoers accountable.

The Organisation for Economic Co-operation and Development (OECD) defines an AI system as a *'machine-based system that, for a given set of objectives, makes predictions, recommendations or decisions influencing real or virtual environments.*'[1] This definition adds the requirement that AI systems operate with varying levels of autonomy and may exhibit adaptiveness after deployment.[2] What is common to both definitions is the idea of decision-making driven by an algorithm that operates with degrees of independence from human volition. Interestingly, it is precisely this independence that makes AI legally disruptive.

Like every other thing created by humans, AI has its own imperfections, ranging from defects in the manufacturing, programming, designs to improper usage. When a human errs, liability flows naturally from agency. However, when an algorithm errs, the chain of causation runs across developers, deployers, users, and institutional choices.

India was among the early movers in articulating a national AI strategy. The National Strategy for Artificial Intelligence (2018) released by NITI Aayog positioned AI as a tool for achieving inclusive growth and framed India's aspiration to be an '*AI garage for the developing world.*'[3] However, what we witness nearly seven years after the release of the strategy largely

[1] OECD, *'Recommendation of the Council on Artificial Intelligence'* (OECD/LEGAL/0449, 2019). The OECD defines AI systems as machine-based systems that, for a given set of objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

[2] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM (2021) 206 final, Art 3(1). The definition in the enacted Regulation (EU) 2024/1689 is found at Art 3(1).

[3] NITI Aayog, 'National Strategy for Artificial Intelligence' (Government of India, 2018) <https://www.niti.gov.in> accessed 2 May 2026. India's strategy identified healthcare, agriculture, education, smart cities, and smart mobility as the five priority sectors for AI-led development.

comprises cases emerging from harm or damage caused by AI and affecting the public at large. Most importantly, the question of liability when algorithms cause damage largely remains unresolved. India still lacks a binding law on artificial intelligence to regulate its manufacturing, programming, and operations, and a dedicated regulating body to adjudicate the liability.

This paper highlights the need for building a robust legal framework for the regulation of artificial intelligence. It first surveys the scope and depth of adoption of AI across important sectors in India and subsequently examines the nature and variety of harms caused by AI systems. Against that empirical backdrop, this paper further analyses the legal consequences of those harms under the existing law and confronts the fundamental question of liability in such cases. Lastly, the paper maps the future challenges that any regulatory framework must anticipate, and concludes with a proposed regulatory framework and a set of actionable legislative recommendations.

II. THE EMERGENCE AND USAGE OF AI IN INDIA

Penetration of artificial intelligence into the Indian economy and state machinery is structural. The AI Adoption Report, 2024, issued by the Ministry of Electronics and Information Technology (MeitY), identified six principal sectors witnessing deep integration of artificial intelligence. These include healthcare, financial services, agriculture, education, governance, and law enforcement.[4]

In *healthcare*, AI-driven diagnostic tools are being deployed in both private and government hospitals. Startups like *Niramai* and *Sigtuple* use machine learning for cancer screening and blood-test analysis, respectively. This diagnosis is operating in a regulatory space that the Drugs and Cosmetics Act, 1940, and the Medical Devices Rules, 2017, were never designed to govern. In *financial services*, the working group of the Reserve Bank of India has noted the proliferation of algorithmic credit scoring and AI-driven lending platforms, many of which operate outside the formal regulatory perimeter of the central bank.[5] Using artificial

[4] Ministry of Electronics and Information Technology (MeitY), 'India AI Mission: Report on AI Adoption Across Sectors' (Government of India, 2024). The India AI Mission, launched in March 2024 with an outlay of Rs 10,371 crore, represents the government's principal commitment to AI infrastructure and adoption.

[5] Reserve Bank of India, 'Report of the Working Group on Digital Lending Including Lending Through Online Platforms and Mobile Apps' (RBI, 2021). The report identified systemic risks from AI-driven algorithmic credit scoring, including concerns about explainability and consumer protection.

intelligence, lenders decide who gets loans, and when they discriminate or err in making accurate decisions, applicants are left without any meaningful legal recourse.

In the *judicial sphere*, SUPACE, an initiative by the Supreme Court of India, uses AI to assist judges with legal research and case management.[6] The Kerala High Court in 2025 mandated the use of '*adalat.ai*' for recording of witness deposition in subordinate courts, while simultaneously issuing guidelines prohibiting AI from being used for decision-making or legal reasoning, citing risks of transparency and accountability. India's AI landscape is shaped by the tension between adoption and accountability.

In *governance and law enforcement*, Police and Airport authorities deploy facial recognition technology through projects such as the Automated Facial Recognition System (AFRS) run by the National Crime Records Bureau, without specific statutory authorisation, parliamentary oversight, or judicially established standards.[7] The scale and diversity of this adoption make the legal vacuum not merely inconvenient, but constitutionally vexatious. NITI Aayog's 2021 framework on Responsible AI identified seven guiding principles, such as *safety, equality, inclusivity, privacy, transparency, accountability, and protection of individual rights*. However, these principles aspirational rather than legally binding.

III. HARM AND INJURY CAUSED BY AI: A TYPOLOGY

The harms caused by AI systems are diverse in nature, diffuse in causation, and often invisible in the conventional legal sense. Unlike a defective product that injures a consumer, AI-driven harm can be systemic, statistical, and distributed across thousands of individuals simultaneously. This makes it resistant to the individualised approach of tort law.

A. Discriminatory and Biased Harm

Perhaps the most pervasive category of AI harm is algorithmic discrimination, where a system trained on historically biased data perpetuates and amplifies those biases in

[6] Supreme Court Portal for Assistance in Court's Efficiency (SUPACE), Ministry of Law and Justice, Government of India (2021). See also Standing Committee on Finance, 'Fourteenth Report: Artificial Intelligence and Financial Markets' (Lok Sabha Secretariat, 2023).

[7] Internet Freedom Foundation, 'Project Panoptic: Tracking Facial Recognition Deployments in India' (2023)
<https://panoptic.in> accessed 1 April 2025. The project has documented over 124 facial recognition technology deployments across India, of which a majority lack any statutory basis.

consequential decisions. The landmark ProPublica study of the COMPAS found that it had about twice the false-positive rate of being future criminals for Black defendants.[8] India is not immune to this risk. Indian case law, social records, and criminal justice data are saturated with biases of caste, religion, gender, and class. AI systems trained on this data will reproduce these biases at scale and with the veneer of algorithmic objectivity.

B. Reputational and Economic Harm

AI-generated deepfakes represent a rapidly escalating category of reputational harm. Indian courts have already confronted this threat directly. In the case of *ANI Media Pvt Ltd v. OpenAI Inc.* (2024),[9] the Delhi High Court admitted India's first AI copyright infringement suit, where a major news agency alleged that its content had been scraped without authorisation to train Large Language Models (LLMs).

In *Dr Devi Prasad Shetty v. Medicine Me* (2024),[10] the Delhi High Court granted an injunction against deepfake videos that exploited a senior cardiac surgeon's likeness to promote fraudulent medical products. These cases reveal that existing law can respond, but only reactively, and only when plaintiffs have enough resources to bring their claims to the court. The systematic harm to ordinary people who experience voice cloning, face fabrication, and reputation destruction remains largely unaddressed.

C. Constitutional Rights Violations

The most serious category of AI harm occurs when they violate constitutionally protected rights. In the landmark case of *K.S. Puttaswamy v. Union of India* (2017)[11], the Supreme Court recognised that the right to privacy is a fundamental right under Article 21 of the Constitution of India. Privacy is invaded by AI systems engaged in mass surveillance, behavioural profiling, and facial recognition without the informed consent of the stakeholders. They also implicate the right to equality under Article 14 when biased algorithms produce

[8] Julia Angwin and others, 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks' (ProPublica, 23 May 2016).
[9] ANI Media Pvt Ltd v. OpenAI Inc., CS(COMM) 1028/2024 (Delhi High Court, 2024). This is India's first reported AI-related copyright infringement action. The plaintiff alleged that OpenAI's large language models were trained on copyrighted news content scraped without authorisation from the plaintiff's website and through its subscribers' licensed reproductions.
[10] Dr Devi Prasad Shetty v. Medicine Me, CS(COMM) 619/2024 (Delhi High Court, 2024). The Delhi High Court granted an ex parte ad interim injunction restraining the defendants from creating and circulating AI-generated deepfake videos misusing the plaintiff's likeness to promote dubious drugs and medical treatments.
[11] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. The nine-judge bench of the Supreme Court of India unanimously held that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21, and more broadly, of the freedoms guaranteed in Part III of the Indian Constitution.

discriminatory outcomes, and the right to a fair trial under Articles 20 and 21, when AI tools assist judicial decision-making without sufficient checks and balances.

A disruptive and highly concerning trend has also surfaced recently across global jurisdictions: the submission of phantom case laws[12]. Advocates are increasingly using unverified and perfectly formatted citations for judgments that simply do not exist and using the same as precedents. This poses a blatant misconduct by the advocates that may invite serious legal consequences for the advocates and parties involved.

D. Physical Harm

Where AI systems operate in the physical world - autonomous vehicles, AI-assisted surgery, and drone delivery, the potential for physical harm is direct and severe. A misclassification by a collision-avoidance system, an incorrect dosage recommendation by a clinical AI, or a targeting error by an AI-guided drone can cause death or grievous injury. The Indian Motor Vehicles Act, 1988, and the Drugs and Cosmetics Act, 1940, are ill-suited for AI-led automation.

In a shocking and deeply unsettling case, a 22-year-old man from Lucknow, Uttar Pradesh, allegedly took his own life after seeking guidance from an artificial intelligence (AI) chatbot[13]. Incidents like these trigger very deep questions about digital ethics, emotional dependency on technology, and the accountability of AI developers when virtual interactions lead to tragic outcomes.

IV. CONSEQUENCES OF AI-DRIVEN HARM

The consequences of AI-driven harm extend well beyond the immediate victim. At the *individual level*, victims face the compounded challenge that AI harm is often difficult to detect, attribute, and remedy. A person denied a loan by an algorithmic credit-scorer may not know why the decision was made, cannot access the AI model's reasoning, and lacks statutory rights to human review in India. A person falsely identified by a facial recognition system at a checkpoint faces detention, reputational damage, and a legal system that struggles to attribute fault to a software-generated output.

[12] Himanshu Mishra, *'Phantom Precedents: The rise of AI-Generated caslackse law in Indian Courts*' (March 17th, 2026) LiveLaw.
[13] *AI Helped Youth Find Ways to Die: Lucknow Family's Complaint Opens Debate on Tech and Mental Health Risks*, Economic Times (May 7, 2026).

At the *institutional level*, the proliferation of unregulated AI creates systemic risk. Financial regulators face the prospect of AI-driven market manipulation, while Judicial institutions face the erosion of public confidence if algorithmic tools influence case outcomes without transparency. Public health authorities face the risk of mass misdiagnosis if AI-based diagnostic tools are deployed without clinical validation standards.

At the *constitutional level*, the absence of accountability frameworks for deploying or using AI creates a structural problem. When the state deploys a biased facial recognition system that systematically misidentifies members of a minority community, it violates fundamental rights, not just tortious duties. Yet, under existing law, there is no mechanism for systematic redress, no institutional auditor of government AI, and no standard of proportionality review applied to algorithmic state action.

V. LIABILITY AND ACCOUNTABILITY: WHICH PARTY IS RESPONSIBLE?

The question of liability for AI-driven harm is perhaps the most technically demanding in all of technology law. It requires disaggregating the AI value chain, which runs from training data collectors, to model developers, to system integrators, to deploying enterprises, to end users, and assigning legal responsibility at each node.

A. Fault-Based Liability: The Limits of Negligence

Classical negligence requires establishing a duty of care, a breach of that duty, causation, and damage. Each element strains when applied to AI. Even if such a duty exists, proving breach is extraordinarily difficult when the defendant's system is a deep learning model whose internal reasoning is opaque even to its creators. Further, establishing that the AI's decision, rather than some intervening human choice, caused the harm, is often impossible to prove.

B. Strict Liability and the Absolute Liability Doctrine

A more promising avenue is strict liability, where liability lies without the need to prove fault. In Indian law, the Supreme Court evolved the principle of absolute liability in *M.C. Mehta v. Union of India* (1987),[14] holding that enterprises engaged in inherently dangerous

[14] M.C. Mehta v. Union of India (1987) 1 SCC 395. The Supreme Court, per P.N. Bhagwati CJ, held that an

activities causing harm to others are absolutely liable for that harm, with no exceptions. This doctrine could possibly apply to certain categories of AI deployment where algorithmic systems cause demonstrable harm. It eliminates the need to prove fault, which simplifies liability. However, as the doctrine targets localized physical damage, lawmakers must clarify how it applies to dispersed, statistical, and cross-border AI harms.

C. A Shared Liability Model for the AI Value Chain

This paper argues that neither pure fault-based liability nor pure strict liability is adequate for AI-induced harm. What is needed is a shared liability model calibrated to the structure of the AI value chain. Under such a model, *developers* bear primary liability for design defects, model bias, and inadequate safety testing; *deployers* bear liability for inappropriate use cases, failure to conduct pre-deployment risk assessments, and absence of human oversight mechanisms. Lastly, *state actors* bear liability where government-deployed AI violates fundamental rights.

MeitY's 2025 AI Governance Guidelines gesture towards this tripartite accountability structure, distinguishing between developers, deployers, and users. However, Guidelines are not law and therefore do not create enforceable rights or compensation, nor bind courts; their main shortcoming is the lack of statutory authority.

VI. THE GLOBAL REGULATORY LANDSCAPE: LESSONS FOR INDIA

A. The European Union AI Act (Regulation (EU) 2024/1689)

The EU AI Act, which entered into force on 1 August 2024[15] is the world's first comprehensive legal framework for AI. Its key architectural feature is its risk-based design. The Act classifies AI systems into four tiers: *unacceptable risk* (prohibited outright); *high risk* (stringently regulated); *limited risk* (transparency obligations only); and *minimal risk* (largely unregulated).

Prohibited AI systems under Article 5 include social scoring systems operated by public authorities, real-time remote biometric identification in public spaces, and AI that exploits cognitive vulnerabilities to manipulate human behaviour.[16] High-risk systems must undergo

enterprise engaged in a hazardous or inherently dangerous activity that causes harm to anyone must be held absolutely liable to compensate for such harm, without any of the exceptions that the rule in Rylands v. Fletcher [1868] LR 3 HL 330 would admit.

[15] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689. The Act entered into force on 1 August 2024. Prohibited practices became applicable from 2 February 2025.

[16] EU AI Act (n 16), Art 5. The prohibited practices include AI systems that deploy subliminal techniques beyond

conformity assessments and human oversight. They also have transparency duties and must be registered in a public EU database. For general-purpose AI models such as LLMs, the EU AI Act, 2024, imposes copyright compliance obligations and technical documentation requirements, and for models with systemic risk, mandatory red-teaming and incident reporting to the European AI Office is prescribed.

B. The United States: Sectoral Flexibility and Executive Action

Instead of comprehensive legislation, the United States uses Executive Orders and agency guidance. Former President, Joe Biden's Executive Order on Safe, Secure, and Trustworthy AI (2023)[17] directed federal agencies to establish AI safety standards and required developers of powerful AI models to share safety test results with the government. The US approach prioritises flexibility and innovation, but its reliance on voluntary frameworks and executive action, without binding statutory force, is its prime weakness, and a cautionary model for India.

C. OECD Principles and the Council of Europe Convention

The OECD's Recommendation on Artificial Intelligence articulates five value-based principles: *inclusive growth; respect for human rights and democratic values; transparency and explainability; robustness, security, and safety; and accountability*.[18] India is a partner to OECD and has endorsed these principles, a fact that makes the absence of binding domestic implementation all the more conspicuous.

The Council of Europe's Framework Convention on AI, Human Rights, Democracy and the Rule of Law (2024), the world's first binding international AI treaty, establishes positive obligations on state parties to ensure that AI systems are consistent with human rights standards. While India is not a signatory, the Convention signals the direction of global normative consensus and the standard against which India's domestic framework will increasingly be measured.

---

a person's consciousness, AI that exploits specific vulnerable groups, AI for social scoring by public authorities, and real-time remote biometric identification systems in publicly accessible spaces for law enforcement (with limited exceptions).

[17] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110), 88 Fed Reg 75191 (30 October 2023) (United States). See also National Institute of Standards and Technology (NIST), 'AI Risk Management Framework' (NIST AI RMF 1.0, January 2023).

[18] OECD, 'Recommendation of the Council on Artificial Intelligence' (n 1). The five OECD AI principles, first adopted in 2019 and updated in 2024, are now endorsed by over 46 countries, including India.

VII. THE INDIAN LEGAL FRAMEWORK: A SYSTEMATIC DIAGNOSIS OF GAPS

India's existing statutory landscape was designed for a world of human actors, physical products, and identifiable perpetrators. When applied to artificial intelligence, each instrument reveals characteristic and significant gaps.

A. The Information Technology Act, 2000

The IT Act 2000, India's foundational digital legislation, provides civil and criminal remedies for a range of cyber offences. Sections 43 and 66 address unauthorised access, data theft, and damage to computer systems. Section 72 penalises breach of confidentiality, and Section 79 provides an intermediary safe harbour - a provision whose application to AI developers and deployers is deeply contested. The IT (Intermediary Guidelines) Amendment Rules of November 2025[19] introduced India's first explicit statutory obligations regarding AI-generated synthetic media. Yet the IT Act, 2000, lacks a definition of AI, standards for algorithm design, mechanisms for algorithmic accountability, or any right to challenge automated decisions. The Act focuses on network security rather than algorithmic oversight.

B. The Digital Personal Data Protection Act, 2023

The DPDP Act, 2023[20], is India's most significant recent contribution to digital law. It imposes obligations on Data Fiduciaries to process personal data lawfully, obtain consent, ensure data accuracy, and maintain security safeguards. However, the Act is entirely silent on automated decision-making. It does not provide a right to explanation, unlike Article 22 of the GDPR, which gives individuals the right not to be subject to purely automated decisions that produce significant effects on them. It does not require algorithmic impact assessments neither addresses the use of personal data for AI training. The DPDP Act is a data protection statute, not an AI governance instrument, and the gap between the two is significant.

C. The Consumer Protection Act,2019

The Consumer Protection Act, 2019, and its product liability provisions under Chapter

[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, published by MeitY on 22 October 2025 and brought into force on 15 November 2025. The amendment introduced explicit statutory obligations on intermediaries with respect to AI-generated synthetic media, including deepfakes.
[20] Digital Personal Data Protection Act 2023 (India) (No. 22 of 2023), ss 4, 6, 7, 8, 9. The Act received Presidential assent on 11 August 2023, but its substantive provisions are subject to a phased commencement notified by the central government. The Act establishes the Data Protection Board of India as the adjudicatory body.

VI impose liability on manufacturers and service providers for defective products and deficient services. However, 'product' under the Act is not defined to include software or AI systems. An AI diagnostic tool that misdiagnoses a patient is likely not a 'product' for the purposes of the Act, or a credit-scoring algorithm that systematically discriminates against a class of borrowers does not obviously constitute a 'deficient service'. These interpretive questions remain unresolved by courts, and the legislature has not addressed them.

D. Tort Law: How far useful?

India's tort law comes from English law and has evolved through court rulings. It provides remedies for negligence, nuisance, and strict liability. The potential for its creative application to AI harms exists, and the doctrine of absolute liability could be extended to AI systems deployed for inherently dangerous purposes. But tort law suffers from structural limitations in the AI context: it is reactive rather than preventive and operates case-by-case rather than systemically. It also demands individualised proof of causation that algorithmic harm often cannot satisfy, and imposes litigation costs that most victims cannot bear. Tort law is a complement to regulation, not a substitute for it.

India currently lacks a specialized AI regulator, statutory liability rules for AI-driven harm, mandatory pre-deployment risk assessments for high-stakes AI systems, a right to explanation for individuals affected by automated decisions, a mandatory algorithmic audit regime, and a compensation fund for AI victims. The AI Governance Guidelines 2025 are advisory, and the Artificial Intelligence (Ethics and Accountability) Bill 2025[21] is a Private Member's Bill without legislative majority. The anticipated Digital India Act[22], which may incorporate AI provisions, remains in a consultative draft. The legal architecture that India's AI economy urgently requires does not yet exist.

VIII. FUTURE CHALLENGES: WHAT ANY GOVERNANCE FRAMEWORK MUST ANTICIPATE

Modern AI systems, particularly deep neural networks, operate in ways that are opaque even to their creators. The concept of 'explainability', the capacity of an AI system to provide

[21] Artificial Intelligence (Ethics and Accountability) Bill 2025 (Private Member's Bill introduced in the Parliament of India, December 2025). The Bill proposes an AI regulatory authority and a statutory ethics framework for AI, but has not been taken up by the government or passed into law.

[22] Digital India Act (proposed), Ministry of Electronics and Information Technology, Government of India. Draft consultations were ongoing through 2024-2026. The DIA, intended to replace the Information Technology Act 2000, is expected to include provisions on AI systems, algorithmic accountability, and deepfake regulation, among other digital law reforms.

a human-intelligible account of its decisions, is both a technical challenge and a legal necessity. Legal systems premised on reasoned decisions and the right to be heard cannot accommodate black-box adjudication.[23] Any Indian AI governance framework must mandate explainability standards for AI systems used in high-stakes contexts, mirroring the transparency requirements in Articles 13 and 14 of the EU AI Act, 2024.

AI systems routinely cross jurisdictional borders. A large language model trained in the United States, deployed by a company registered in Singapore, used by Indian consumers, and causing harm to Indian citizens, presents a jurisdictional maze that domestic law is not equipped to navigate. India needs domestic laws with extraterritorial effect on the model of the applicability of the DPDP to offshore Data Fiduciaries, along with active engagement with international AI governance forums to negotiate common standards and mutual enforcement mechanisms.

Further, the technical complexity of AI regulation creates a persistent risk of regulatory capture: a scenario where the regulator, for want of technical expertise, defers excessively to the industry it is meant to oversee. India's experience with data protection regulation, where implementation has lagged years behind the statute, is a cautionary precedent. Any AI regulator must be staffed with engineers and data scientists as well as lawyers, and insulated from industry capture through robust conflict-of-interest standards and transparent appointment processes.

Perhaps the gravest long-term challenge is the use of AI by the state itself. When the state uses AI for surveillance, predictive policing, welfare allocation, or judicial assistance, the risks are not merely those of inefficiency or error; they are risks to the constitutional order. The proportionality doctrine developed in the *Puttaswamy* case requires that any state interference with fundamental rights be proportionate to a legitimate aim and subject to procedural safeguards. Applying this doctrine to state AI deployments demands, at a minimum, a statutory basis for each use case, an independent audit of the system's accuracy, and a mechanism for affected individuals to seek review.

[23] Gary Marcus and Ernest Davis, Rebooting AI: Building Artificial Intelligence We Can Trust (Pantheon Books 2019) 173-195. The challenge of explainability in deep learning systems, often described as the 'black box' problem, is a central concern in both AI ethics and AI law literature.

IX. RECOMMENDATIONS: A BLUEPRINT FOR INDIAN AI GOVERNANCE

A. Enact a Standalone AI Regulation Act with Risk-Tiered Classification

First and foremost, India should enact a standalone AI Regulation Act structured around a four-tier risk classification, modelled on but adapted from the EU AI Act, 2024, to reflect India's constitutional framework and developmental context:

(i) **Prohibited AI (Tier 0):** AI systems for social scoring by state authorities, real-time biometric mass surveillance in public spaces, and AI designed to subliminally manipulate electoral behaviour should be prohibited outright by statute.

(ii) **High-Risk AI (Tier 1):** AI systems in criminal justice, healthcare diagnostics, financial credit assessment, welfare eligibility, and government surveillance should be subject to mandatory pre-deployment conformity assessments, algorithmic impact assessments, explainability requirements, human oversight mandates, and registration with the National AI Regulatory Authority.

(iii) **Moderate-Risk AI (Tier 2):** AI systems interacting with citizens in service delivery and consumer-facing applications should be subject to transparency obligations, including disclosure of AI involvement and the right to request human review of significant decisions.

(iv) **Low-Risk AI (Tier 3):** Systems such as spam filters and entertainment recommendation engines should operate under voluntary codes of conduct without mandatory pre-market requirements.

B. **Establish a National AI Regulatory Authority**

India should establish a National AI Regulatory Authority (NAIRA) as a statutory, independent body with the following institutional mandate: registration and certification of Tier 1 and Tier 2 AI systems before deployment; ongoing monitoring and audit of deployed high-risk AI systems; investigation of AI-driven harm complaints from individuals and organisations; imposition of civil penalties and mandatory remediation orders; and publication of algorithmic impact assessment reports for government AI deployments.

NAIRA should be constituted with a multi-disciplinary board comprising legal experts, data scientists, ethicists, civil society representatives, and sectoral specialists. Sector-specific coordination councils - for health AI, financial AI, and judicial AI, respectively- should operate under NAIRA's umbrella. Crucially, NAIRA must be insulated from regulatory capture through

fixed-term appointments, transparent public hearings, and an obligation to publish reasoning for all regulatory decisions.

C. Legislate a Shared AI Liability Framework

The AI Regulation Act should include a dedicated Chapter on AI Liability establishing the following principles of shared responsibility across the AI value chain: *developers* of high-risk AI systems bear strict liability for design defects and model failures causing demonstrable harm, unless they demonstrate compliance with mandatory pre-market safety standards; *deployers* bear liability for harms arising from inappropriate use cases, failure to implement mandatory human oversight, or deployment in contexts for which the system was not certified; *intermediaries* hosting AI-generated harmful content incur liability where they fail to act on verified complaints within a prescribed timeframe; and the *State* bears constitutional tort liability for fundamental rights violations caused by government-deployed AI systems, enforceable through writ jurisdiction.

D. Amend the DPDP Act, 2023, to Include AI-Specific Rights

The DPDP Act, 2023 should be amended to include: a right to explanation for any individual subject to a solely automated decision with significant effects; a right to human review of such decisions in specified high-stakes categories; a prohibition on automated decisions in criminal justice and welfare allocation without mandatory human oversight; and an obligation on Data Fiduciaries using personal data for AI training to disclose this purpose explicitly at the point of consent collection.

E. Mandate Algorithmic Impact Assessments for Government AI

By legislative provision or executive mandate, all government ministries and public authorities deploying AI systems should be required to conduct and publish Algorithmic Impact Assessments before deployment. Such assessments should evaluate: the system's stated purpose and likely actual effects; accuracy and error rates disaggregated by gender, religion, caste, and socioeconomic status; the potential for fundamental rights violations; and the mechanism for individual redress.

X. CONCLUSION

India stands at a crossroads in its relationship with artificial intelligence. It can adopt a regulatory framework that protects rights, or continue with a governance vacuum where AI systems are deployed at scale, and harms accumulate without legal remedy. India's existing legal architecture, including the IT Act, 2000, the DPDP Act, 2023, the Consumer Protection Act, 2019, and the common law of torts, is structurally inadequate to govern the AI systems now operating within its borders. The inadequacy is not peripheral but fundamental, as these statutes do not assign liability through the AI value chain.

India has the institutional capacity, the constitutional framework, and the jurisprudential foundation to build a world-class AI governance architecture. India needs both political will and faster legislation to prevent AI-induced harm now. The harms of unregulated AI do not wait for parliamentary schedules. They are accumulating now, in discriminatory credit decisions, in biased predictive policing, in deepfake reputational attacks, in opaque government algorithms determining access to welfare, and in surveillance systems that operate without legal authority.

The enactment of a comprehensive AI Regulation Act, the establishment of a National AI Regulatory Authority, the amendment of the DPDP Act, 2023, to include AI-specific rights, and the adoption of a shared liability framework across the AI value chain are not aspirational goals, but constitutional necessities. A legal system built on the promise of equality, dignity, and accountability cannot afford to leave artificial intelligence ungoverned.