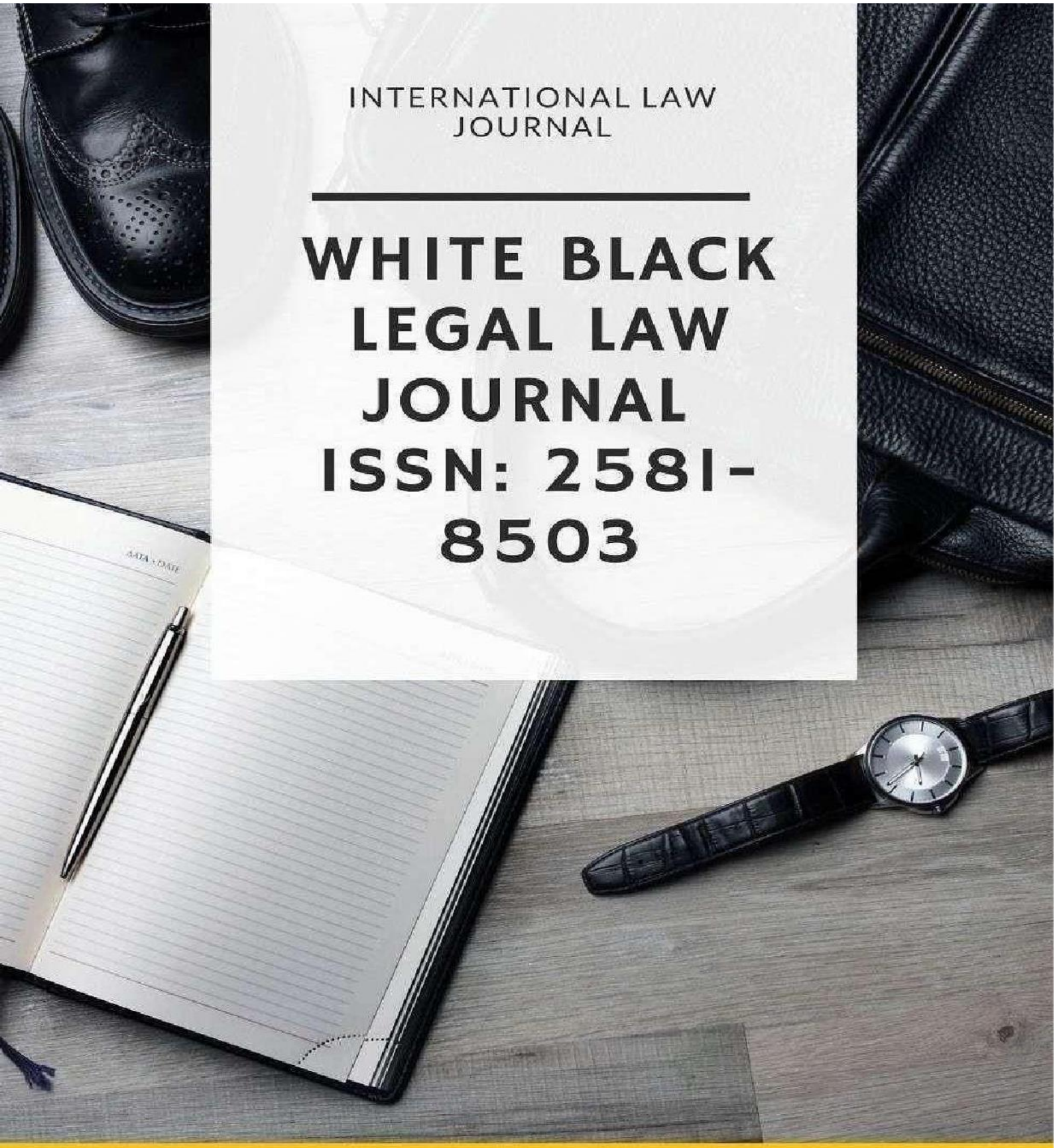

INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

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.

WHITE BLACK LEGAL

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.

www.whiteblacklegal.co.in
Volume 2 Issue 16 | 1 July 2024 ISSN: 2581-8503

NAVIGATING THE ALGORITHMIC FRONTIER: ARTIFICIAL INTELLIGENCE AND THE EVOLUTION OF INDIAN LAW

AUTHORED BY - TUSHAR CHAUDHARY
Law Centre-I, Faculty of Law, University of Delhi.

ABSTRACT

The rapid evolution of Artificial Intelligence (AI) has shifted it from a futuristic technological novelty into a core socio-economic and legal reality. In India, a jurisdiction defined by its burgeoning digital ecosystem and massive data generation, the intersections between advanced algorithmic systems and existing legal structures present deep constitutional, regulatory, and systemic challenges. This paper provides a comprehensive analysis of the Indian legal framework concerning AI as of 2026. It traces the doctrinal progression of AI governance from early soft-law policies, such as the NITI Aayog's "Responsible AI for All" strategies, to contemporary hard-law intersections, specifically the Digital Personal Data Protection (DPDP) Act, 2023, and emerging sector-specific mandates. The paper examines critical areas of friction: the liability paradox in civil, criminal, and corporate governance regimes; the shifting paradigms of intellectual property rights involving AI-generated works and machine-learning data scraping; and the integration of predictive algorithms within law enforcement and judicial administration. Through a comparative analysis alongside the European Union's AI Act and United States frameworks, this study highlights structural and statutory gaps within Indian law. It concludes by proposing a balanced, risk-tiered regulatory framework engineered to preserve constitutional guarantees, protect public welfare, and foster technological innovation within the Indian digital economy.

1. Introduction: The Socio-Technical Context of AI in India

The global landscape of computational technology has experienced a paradigm shift driven by deep learning networks, large language models (LLMs), and autonomous decision-making agents. India has emerged as a critical focal point in this technological evolution. Benefiting from massive digital adoption, state-supported public digital infrastructure (such as the Unified Payments Interface and Aadhaar), and a vast base of tech consumers, the country generates an

unprecedented volume of data (Joshi, 2024). This extensive data environment serves as an ideal training ground for sophisticated AI architectures, accelerating innovation across sectors like healthcare, finance, corporate governance, and criminal justice (Khalique et al., 2026).

However, these socio-technical developments pose significant challenges to traditional legal systems. The Indian legal framework, inherited largely from common-law traditions and built upon human-centric doctrines of intent, causation, and agency, struggles to absorb systems characterized by opacity—the "black box" phenomenon—and relative autonomy. When an algorithm autonomously generates a medical misdiagnosis, executes an anti-competitive market strategy, produces defamatory or fabricated legal text, or conducts biased profiling in predictive policing, traditional statutes like the Law of Torts, the Indian Penal Code (now *Bharatiya Nyaya Sanhita*), and the Information Technology Act, 2000, face operational limits.

This research paper evaluates the relationship between Indian law and artificial intelligence. It maps how existing legislative provisions adapt to automated technologies, identifies systemic enforcement and statutory gaps, and builds a conceptual model for a dedicated legislative framework that balances technological advancement with the constitutional guarantees of the Indian Republic.

2. Historical Trajectory of AI Policy and Governance in India

The evolution of AI governance in India can be divided into two distinct eras: an initial phase focused on promotional policies, followed by a more recent shift toward regulatory accountability.

2.1 The Soft Law Approach: NITI Aayog's National Strategies

For a long time, the Indian government avoided implementing restrictive, top-down legislative controls on software developers, viewing regulation as a potential drag on economic growth (Marda, 2018). Instead, governance was driven by state-backed think tanks using soft-law frameworks. The foundational step occurred in June 2018, when NITI Aayog published its *National Strategy for Artificial Intelligence: #AIforAll* (Joshi, 2024). This policy positioned India as an experimental space for data-driven technologies, identifying five sectors where AI could drive social inclusion and economic value:

1. **Healthcare:** Increasing access and speed of diagnostics in rural communities.

2. **Agriculture:** Utilizing predictive metrics for crop optimization and water management.
3. **Education:** Implementing personalized adaptive learning platforms.
4. **Smart Cities and Infrastructure:** Developing intelligent systems for traffic and utility networks.
5. **Smart Mobility and Transportation:** Optimizing logistics and mass transit pipelines.

While the 2018 strategy focused primarily on economic potential, NITI Aayog subsequently released a two-part approach titled *Responsible AI for All* between 2020 and 2022 (Joshi, 2024). These documents introduced ethical considerations into Indian policy discussions, outlining core principles such as safety, reliability, equality, non-discrimination, privacy, transparency, and accountability. However, as soft-law instruments, these guidelines lacked enforcement mechanisms, penalties for non-compliance, and statutory backing, leaving ethical adherence entirely to voluntary industry adoption (Joshi, 2024).

2.2 The Transition to Hard Law and Sectoral Regulations

As AI systems grew more widespread, voluntary compliance proved insufficient to handle algorithmic harms like deepfakes, algorithmic bias, financial fraud, and privacy infractions. Consequently, various ministries began shifting toward binding administrative and statutory regulations.

The Ministry of Electronics and Information Technology (MeitY) utilized its rule-making powers under the Information Technology Act, 2000, to issue advisories targeting generative AI platforms, requiring companies to ensure their models did not spread misinformation or disrupt democratic processes. Simultaneously, specialized regulators stepped in. The Reserve Bank of India (RBI) introduced strict guidelines regarding algorithmic scoring models used in fintech lending, demanding clear accountability for automated credit assessments. Similarly, the Securities and Exchange Board of India (SEBI) established reporting requirements for algorithmic trading systems to prevent automated market manipulation. This patchwork of responses highlighted a growing regulatory challenge: India was attempting to govern a highly interconnected technology through fragmented, sector-specific rules.

3. Constitutional Imperatives, Privacy, and Data Protection

The integration of AI systems into public and private spaces directly affects fundamental rights protected under Part III of the Constitution of India. Because AI relies heavily on large-scale data collection, its development exists in tension with constitutional privacy protections.

3.1 The Puttaswamy Doctrine and Informational Privacy

The constitutional boundaries for data-intensive technologies were established by the Supreme Court of India in the landmark ruling *Justice K. S. Puttaswamy v. Union of India* (2017). The nine-judge bench unanimously recognized the right to privacy as an intrinsic component of the right to life and personal liberty under Article 21 of the Constitution. The Court explicitly identified "informational privacy" as a protected right, noting that individuals retain an interest in digital profiles generated by algorithms.

The *Puttaswamy* judgment established a strict three-fold test to validate any state action that infringes upon individual privacy:

- **Legality:** The action must be backed by an explicit statutory law.
- **Need/Legitimate State Aim:** The measure must serve a valid public interest goal.
- **Proportionality:** The state must adopt the least intrusive method available, ensuring a rational connection between the objective and the means employed.

Many public-sector deployments of AI—such as state-wide automated facial recognition networks used for crowd surveillance or predictive policing systems—struggle to satisfy this three-part test (Gupta & Bharadwaj, 2023). Often deployed via administrative orders rather than clear legislative acts, these systems lack specific statutory authorization and can fail to meet constitutional standards for necessity and proportionality.

3.2 The Digital Personal Data Protection (DPDP) Act, 2023, as a Regulator of AI

The long-awaited statutory response to the *Puttaswamy* mandate arrived with the passage of the Digital Personal Data Protection (DPDP) Act, 2023. While not explicitly framed as an "AI Regulation Act," the DPDP Act functions as a primary legal constraint on AI developers operating in India, as AI models require extensive personal data for training, fine-tuning, and deployment.

The DPDP Act reshapes the operational landscape for AI systems through several core mechanisms:

- **The Consent Architecture (Sections 5 & 6):** AI systems can process personal data only for specified, lawful purposes based on explicit, unambiguous, and revocable consent from the "Data Principal" (the individual), or under specific "legitimate uses." This limits the common practice of scraping public web sources for personal data to train generative AI models without individual authorization.
- **Purpose Limitation and Data Minimization (Section 7):** AI platforms are legally barred from processing personal data beyond the specific purpose for which consent was

granted. If an AI app collects behavioral metrics to optimize user experience, it cannot repurpose that information to train a commercial predictive credit algorithm without separate consent.

- **Obligations of Significant Data Fiduciaries (Section 10):** The Central Government can designate certain entities as Significant Data Fiduciaries (SDFs) based on factors like the volume of data handled and risks to public order. Large-scale AI developers classified as SDFs face additional compliance burdens, including mandatory Data Protection Impact Assessments (DPIAs), independent data audits, and the appointment of an India-based Data Protection Officer.
- **Cross-Border Data Flows (Section 16):** While the DPDP Act allows for a more flexible data-transfer model compared to earlier drafts, it empowers the government to restrict or blacklist specific jurisdictions from receiving personal data belonging to Indian citizens. This restriction directly impacts international cloud infrastructure and cross-border AI training pipelines.

Despite these protections, the DPDP Act features a significant structural gap regarding AI governance: it lacks a dedicated mechanism addressing automated decision-making. Unlike the European Union's General Data Protection Regulation (GDPR), which grants citizens a specific right not to be subject to solely automated profiling that carries legal effects, the Indian DPDP Act does not explicitly address automated profiling or mandate human-in-the-loop overrides.

4. The Liability Paradox: Civil, Criminal, and Corporate Governance

A central challenge in adapting common-law jurisprudence to AI involves assigning legal liability when an autonomous system causes harm. Common law relies on proving a chain of causation linked to human negligence, recklessness, or malicious intent—concepts that can break down when applied to advanced algorithmic decisions.

4.1 Tortious and Civil Liability: Negligence vs. Strict Liability

When an AI-driven system causes financial loss, property damage, or physical injury, injured parties typically seek redress under the Law of Torts. However, applying the standard test for negligence presents clear evidentiary hurdles.

Proving a breach and proximate causation becomes exceptionally difficult due to the "black box" nature of deep neural networks. If a clinical AI tool misses a malignant tumor on an X-ray, the hospital can argue it exercised standard care by using certified software. Meanwhile,

the software developer can show that the model was trained on high-quality historical data, making the error an unpredictable emergent property of a complex system rather than a coding error.

To resolve this challenge, Indian legal scholars are looking toward the doctrine of **Strict Liability**, established in English law by *Rylands v. Fletcher* (1868) and adapted for India as **Absolute Liability** by the Supreme Court in *M.C. Mehta v. Union of India* (1987). Under absolute liability, an entity engaged in an inherently hazardous or dangerous activity is held accountable for any resulting harm, regardless of intent or precautions taken.

Applying this framework to AI involves treating the operation of autonomous systems in critical infrastructure (such as self-driving transit networks, automated industrial grids, and surgical robotics) as an inherently hazardous activity. This shifts the legal focus from proving fault to managing systemic risk, ensuring that the enterprise profiting from the deployment bears the cost of its failures.

4.2 Criminal Liability: Actus Reus and Mens Rea without a Human Actor

Indian criminal law, governed by the *Bharatiya Nyaya Sanhita* (BNS), requires two elements to establish criminal culpability: *actus reus* (the prohibited physical act) and *mens rea* (the guilty mind or criminal intent).

While an autonomous system can execute actions that lead to a prohibited outcome—such as executing an unauthorized financial trade or generating defamatory text—an algorithm lacks consciousness and cannot form a guilty mind. As a result, an AI system cannot be held directly liable under current criminal statutes (Chaudhary, 2020).

Consequently, criminal liability must be traced back to human actors using established modes of secondary liability:

- **The AI as an Innocent Agent:** If a human user deploys an AI tool with the explicit intent to commit a crime (e.g., configuring an LLM to generate targeted spear-phishing scripts), the human user is held liable as a principal offender. The AI is treated simply as an instrument, analogous to a physical weapon.
- **Criminal Negligence:** If a software developer releases an autonomous system while ignoring known safety flaws or omitting critical adversarial testing, they can be prosecuted for criminal negligence under sections of the BNS governing rash or negligent acts that endanger human life.
- **The Corporate Fit:** For complex, corporate-driven deployments, liability can be established by adapting the doctrine of corporate criminal liability. Criminal intent can

be attributed to the company by showing that its executives or board authorized the deployment of an unstable or unverified system for commercial gain.

4.3 Corporate Governance: AI in the Indian Boardroom

The integration of AI into corporate management introduces distinct challenges regarding corporate governance and fiduciary responsibilities under the Companies Act, 2013. Venture capital funds and technology companies have experimented with utilizing analytical AI systems to assist, or even vote on, investment strategies and operational decisions (Baburaj).

Under Section 149 of the Indian Companies Act, 2013, only a natural human individual can be formally appointed as a director to a company's board (Baburaj). This statutory requirement preserves clear personal accountability, ensuring that directors cannot delegate their legal responsibilities to software solutions (Baburaj).

Section 166 of the Act outlines the specific fiduciary duties of directors, mandating that they act in good faith, with independent judgment, and with due and reasonable care, skill, and diligence. This creates a dual challenge for directors interacting with AI tools:

- **Over-Reliance (The Automation Bias):** If a board blindly approves an expensive acquisition or restructuring plan based solely on automated algorithmic projections without conducting independent due diligence, the directors may be found in breach of their statutory duty to exercise independent judgment.
- **Under-Reliance (Technological Blindness):** In highly competitive markets, if a board ignores clear insights from verified analytical software, leading to substantial preventable losses, shareholders could argue the directors failed to exercise reasonable care and diligence.

To meet their duties under Section 166, corporate directors must maintain a balanced approach: utilizing AI tools as analytical supplements while retaining final, independent decision-making authority.

5. Intellectual Property Rights (IPR) in the Era of Machine Intelligence

The growth of generative AI challenges traditional frameworks of intellectual property law, which were designed around human creativity and labor.

5.1 Copyright Law: The Authorless Creation Dilemma

The Indian Copyright Act, 1957, faces challenges from AI-generated creative outputs,

including code, digital art, literature, and music. Section 2(d) of the Act explicitly defines the "author" of a work as the human individual who caused the creation to be made. For computer-generated works, it points to the person who created the conditions for its production.

This statutory definition creates a clear legal divide based on the level of human involvement:

- **AI-Assisted Works:** When a human creator uses an AI tool as a supplement—similar to an editor or design software—while exercising clear creative choice over the final structure, copyright protection is generally maintained. The human remains the author.
- **AI-Generated Works:** When a user enters a brief text prompt and an autonomous system generates the entire final work, the system lacks a human author. Because an algorithm cannot hold legal property rights under Indian law, these purely automated outputs risk falling outside copyright protection and entering the public domain.

The standard for originality in India was established by the Supreme Court in *Eastern Book Company v. D.B. Modak* (2008). The Court rejected the older English "sweat of the brow" doctrine, which rewarded pure labor, and adopted a standard requiring a "modicum of creativity." The work must exhibit some intellectual effort, judgment, and product differentiation. Because an algorithm executes mathematical optimizations rather than human judgment, its independent outputs do not meet the *Eastern Book Company* standard. Therefore, for an AI-assisted work to receive copyright protection, the human user must demonstrate substantial personal intellectual input in refining and structuring the final output.

5.2 The Fair Dealing Defense vs. Massive Algorithmic Training

A significant global legal battle involves the unauthorized scraping of copyrighted datasets to train commercial AI models. In India, this issue is evaluated under Section 52(1)(a) of the Copyright Act, 1957, which governs the doctrine of **Fair Dealing**.

Unlike the broad, flexible "Fair Use" factors used in the United States, India's Fair Dealing framework uses an exhaustive, purpose-specific list. It explicitly permits unauthorized uses of copyrighted works only for specified tasks, such as private study, research, criticism, review, or news reporting.

Commercial AI developers scraping proprietary databases to train market-facing models struggle to fit within these narrow exceptions. While an argument can be made for models developed purely within academic or non-profit research settings, commercial data scraping without a license likely constitutes an infringement of the copyright holder's exclusive reproduction rights under Section 14 of the Act.

5.3 Patent Law and the Inventor Space

A parallel challenge exists within Indian patent law, governed by the Patents Act, 1970. Sections 2(1)(p) and 6 require that an applicant for a patent must be the "true and first inventor," a definition consistently interpreted by Indian courts and the Patent Office as a natural human being. This view aligns with international decisions, such as those regarding the DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) patent applications. The Indian Patent Office maintains that an AI system cannot be listed as an inventor because it lacks legal personhood and cannot assign or transfer patent rights. Consequently, inventions generated autonomously by AI models remain unpatentable in India unless a human collaborator can demonstrate a primary, directive role in designing the underlying inventive step.

6. AI in the Administration of Justice and Law Enforcement

The deployment of algorithmic systems by law enforcement and judicial authorities introduces distinct institutional risks regarding procedural fairness and human rights.

6.1 Automated Facial Recognition Systems (AFRS) and Surveillance

Law enforcement agencies across India have rapidly integrated Automated Facial Recognition Systems (AFRS) into public policing. Managed by entities like the National Crime Records Bureau (NCRB), these systems scan CCTV feeds in public transit hubs, political demonstrations, and urban spaces to match faces against centralized criminal databases (Gupta & Bharadwaj, 2023).

These deployments introduce several critical legal concerns:

- **The Lack of Specific Statutory Backing:** Many AFRS networks operate under administrative guidelines rather than explicit legislative acts, which challenges the legality requirement established in the *Puttaswamy* privacy framework (Gupta & Bharadwaj, 2023).
- **Algorithmic Bias and High Error Rates:** Global and domestic studies show that facial recognition algorithms exhibit higher error rates when processing women and marginalized groups. A false positive match can lead to improper targeting, detentions, and violations of liberty under Article 21.
- **Function Creep:** Systems originally introduced for narrow purposes, such as tracking missing children, have been repurposed for general public surveillance and identifying

political protestors, creating a chilling effect on the freedoms of speech, assembly, and movement guaranteed under Article 19.

6.2 Predictive Policing and Algorithmic Profiling

Predictive policing involves using historical crime data to train machine-learning models that forecast where crimes are likely to occur or who is most likely to commit them. However, this approach risks codifying historical biases into automated systems. If historical policing data reflects disproportionate surveillance or systemic biases against specific marginalized communities, the algorithm will treat those geographic areas as high-risk zones. This creates a feedback loop: the algorithm directs more officers to those neighborhoods, leading to more arrests, which reinforces the model's initial bias. This automated profiling conflicts with Article 15 of the Constitution, which prohibits discrimination by the State on grounds of religion, race, caste, sex, or place of birth.

6.3 AI in Criminal Sentencing and Legal Practice

Within the judiciary, AI applications have expanded from basic administrative support to advanced analytics. Tools like *SuVas* (Supreme Court Vidhik Anuvaad Software) translate legal documents into regional languages, while *SUPACE* (Supreme Court Portal for Assistance in Courts Efficiency) helps judges sort and analyze case files.

However, incorporating predictive analytics into criminal sentencing or bail determinations introduces significant procedural concerns (Hassan Md, 2024). In other jurisdictions, software like COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) has faced criticism for lack of transparency and biased risk-scoring.

Under Indian law, criminal sentencing requires judges to weigh both aggravating and mitigating factors tailored to the individual offender (Hassan Md, 2024). This individualized assessment requires human empathy, a deep understanding of social context, and a willingness to offer opportunities for rehabilitation—qualities that cannot be replicated by data-driven algorithms (Hassan Md, 2024). If an algorithm dictates a predictive recidivism score without disclosing its underlying data weights, it undermines the principle of a fair trial and limits the judge's sentencing discretion (Hassan Md, 2024).

Furthermore, the use of AI in private legal practice has introduced new professional liabilities. If an advocate relies blindly on an unverified generative AI platform that fabricates legal precedents or contains errors, the lawyer cannot delegate their professional obligations to the technology (Joshi). Under the Advocates Act, 1961, and the Bar Council of India Rules,

submitting unverified, fabricated case law can be treated as professional misconduct, undermining judicial integrity and compromising the client's right to competent representation (Joshi).

7. Comparative Analysis: India, the European Union, and the United States

To design an effective regulatory framework, India can draw valuable insights from the contrasting regulatory models developed by the European Union and the United States.

Regulatory Domain	European Union (EU AI Act)	United States (Decentralized Model)	India (Current Framework)
Primary Philosophy	Rights-centric, precautionary, and strictly rules-based.	Market-driven, sector-specific, and innovation-focused.	Mixed; transitioning from promotion to fragmented control.
Structural Architecture	Unified, horizontal statutory regulation across the EU.	Decentralized; driven by executive orders and sector regulators.	Fragmented; governed by the DPDP Act and individual sectoral policies.
Risk Classification	Four clear tiers: Unacceptable, High, Limited, Minimal.	No uniform statutory classification model.	No formalized statutory risk-tiering matrix.
Enforcement Body	European AI Office and national supervisory authorities.	Split across agencies like the FTC, FDA, and SEC.	Handled across MeitY, sectoral regulators, and the DPBD.

7.1 The European Union Model: The Precautionary Approach

The European Union's AI Act stands as a comprehensive, horizontal legislative framework. It classifies AI systems into four risk-tiered categories:

1. **Unacceptable Risk:** Systems that threaten human safety or rights—such as state-backed social scoring or biometric categorization based on political beliefs—are strictly banned.
2. **High Risk:** Systems used in critical infrastructure, education, employment, and law enforcement face strict compliance obligations, including mandatory conformity

assessments, high-quality training datasets, detailed logging, and human-in-the-loop oversight.

3. **Limited Risk:** Applications like chatbots face clear transparency requirements, ensuring users are informed they are interacting with an AI system.
4. **Minimal Risk:** Standard applications like video games face no additional regulatory burdens.

The EU model prioritizes consumer protection and fundamental human rights, using heavy financial penalties to enforce compliance. However, critics argue this rigid framework imposes high compliance costs that can stifle early-stage startups and slow down broader innovation.

7.2 The United States Model: Market Innovation and Executive Direction

The United States has avoided passing a singular, comprehensive federal law governing AI. Instead, it relies on a decentralized, sector-specific model led by existing federal agencies like the Federal Trade Commission (FTC) and the Food and Drug Administration (FDA).

This approach is guided by the *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*. This directive instructs federal agencies to develop safety standards, protect consumer privacy, prevent algorithmic discrimination, and secure critical domestic infrastructure. The US model prioritizes flexibility, technological agility, and market leadership, though it can leave gaps in consumer protection due to varying enforcement across state lines and agencies.

7.3 Strategic Implications for India

India's regulatory path does not require a direct choice between these two approaches. Blindly copying the EU AI Act could burden India's developing software sector with restrictive compliance costs. Conversely, adopting the US model could leave vulnerable populations exposed to algorithmic bias, data exploitation, and unsafe deployments.

Therefore, India's regulatory strategy should blend these models: adopting a clear risk-tiered framework for critical public infrastructure while leaving experimental spaces unregulated to support local innovation.

8. Proposed Regulatory Framework for India: The Way Forward

To address existing statutory gaps, India needs to transition from fragmented sector-specific advisories to a comprehensive, dedicated legislative framework. India should enact a specialized statute: the **Artificial Intelligence (Governance and Accountability) Act**.

8.1 Establishing the Artificial Intelligence Authority of India (AIAI)

The proposed Act should establish a dedicated regulatory body: the **Artificial Intelligence Authority of India (AIAI)**. Operating as an independent, multi-disciplinary agency, the AIAI would include computer scientists, legal scholars, ethicists, and industry representatives.

Rather than replacing existing regulators, the AIAI would serve as a centralized hub to coordinate policy across sectors. It would issue technological standards, certify independent AI auditors, investigate large-scale algorithmic failures, and manage regulatory sandboxes to support early-stage innovation.

8.2 Implementing an Indian Risk-Classification Matrix

Following a risk-tiered approach tailored to India's social context, technologies should be categorized into three levels:

A. Prohibited Systems

Certain applications should be banned because they conflict with the constitutional guarantees of dignity and equality under the Indian Constitution:

- Systems designed to manipulate human behavior in ways that cause physical or psychological harm.
- State-run social scoring infrastructure used to restrict access to public services or constitutional freedoms.
- Real-time untargeted public biometric identification networks, except when authorized by a federal court during a declared national security emergency.

B. High-Risk Systems

Applications that directly affect individual safety, liberty, or fundamental rights must meet strict compliance standards before deployment:

- Automated tools used in healthcare diagnostics, biometric identification, and public utility management.
- Algorithmic scoring tools used for employment screening, university admissions, and credit evaluations.
- Predictive policing software and automated translation systems used within judicial administration.

Developers of high-risk systems would be legally required to perform mandatory pre-deployment Data Protection Impact Assessments (DPIAs), maintain clear system logging for auditability, implement human-in-the-loop overrides, and provide plain-language explanations of their models' decision-making processes to prevent "black box" opaque harms.

C. General and Exempt Systems

Low-risk applications—such as enterprise internal inventory management, consumer entertainment software, creative tools, and spam filters—would be exempt from heavy compliance burdens. They would only need to follow basic transparency standards, such as clearly labeling AI-generated content or synthetic media.

8.3 Statutory Reallocation of Liability

To resolve the liability challenges in civil and corporate law, the proposed statute should update existing liability assignment rules:

- **The Strict Product Liability Model:** For high-risk deployments, the framework should implement a strict product liability model. If an automated system malfunctions due to systemic design flaws or inadequate training data, liability should shift directly to the developer or enterprise platform profiting from the deployment, reducing the burden on injured consumers to prove negligence.
- **The Mandatory Insurance Pipeline:** To protect consumers without halting industry innovation, high-risk AI deployments should be tied to a mandatory third-party liability insurance framework. This setup would ensure injured parties can secure financial recovery while allowing insurance providers to incentivize safety by tying premium costs to verified algorithmic audits.

9. Conclusion

The intersection of Indian law and Artificial Intelligence represents a defining challenge for modern jurisprudence. The existing framework—a combination of common-law liability doctrines, sector-specific guidelines, and the data protection rules of the DPDP Act, 2023—remains fragmented and incomplete when facing the challenges of autonomous, opaque technologies.

Leaving these gaps unaddressed creates a double risk: it leaves individual constitutional rights vulnerable to automated bias and systemic errors, while leaving tech enterprises without the clear rules needed to confidently scale investments.

India's regulatory path requires a balanced framework. By establishing a dedicated Artificial Intelligence Authority of India (AIAI) and implementing a risk-tiered compliance model, India

can protect the fundamental rights guaranteed under its Constitution while providing a clear roadmap for technological growth. This approach ensures that as India develops its digital economy, its technological foundations remain aligned with public welfare, human accountability, and the rule of law.

REFERENCES

- *Baburaj, A. (n.d.). Artificial intelligence v. intuitive decision making: How far can it transform corporate governance? The GNLU Law Review, 8(2), 236–258. Cited by: 5*
- *Chaudhary, G. (2020). Artificial intelligence: The liability paradox. ILI Law Review, Summer Issue 2020, 147–162. https://doi.org/10.2139/ssrn.3709095 Cited by: 18*
- *Eastern Book Company v. D.B. Modak, (2008) 1 SCC 1 (India).*
- *Gupta, K., & Bharadwaj, A. (2023). Facial recognition systems: The confluence of artificial intelligence, privacy & criminal justice. Bennett Journal of Legal Studies, 4(1), 41–55. Cited by: 2*
- *Hassan Md, T. (2024). The perils and promises of artificial intelligence in criminal sentencing. Indian Journal of Law and Technology, 19(2), 1–24. Cited by: 1*
- *Joshi, D. (2024). AI governance in India – law, policy and political economy. Communication Research and Practice, 10(3), 328–339. https://doi.org/10.1080/22041451.2024.2346428 Cited by: 33*
- *Joshi, R. (n.d.). Legal responsibility for AI errors and professional misconduct in India. The Research Dialogue, 1–15. Cited by: 0*
- *Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).*
- *Khalique, N., Nasir, M., Ahmed, S., & Siddiqui, K. (2026). The role of artificial intelligence in improving the public health care delivery system in India: A legal-ethical audit. Journal of Community Medicine, 12(1), 110–125. Cited by: 1*
- *Marda, V. (2018). Artificial intelligence policy in India: A framework for engaging the limits of data-driven decision-making. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133), 20180087. Cited by: 268*
- *M.C. Mehta v. Union of India, AIR 1987 SC 1086 (India).*
- *Rylands v. Fletcher, (1868) LR 3 HL 330 (UK).*