International Journal of Applied Review
www.multiappliedjournal.com
ISSN: 3107-8443
Received: 26-10-2025, Accepted: 25-11-2025, Published: 10-12-2025
Volume 1, Issue 2, 2025, Page No. 49-58

Regulating artificial intelligence in India: Legal frameworks, governance challenges, and the path toward a dedicated AI law

Ganesh Shrirang Satarkar Nale
Department of Sociology, Central University of Haryana, Haryana, India

Abstract
Artificial Intelligence (AI) has emerged as a transformative technology reshaping governance, economy, and social interactions across the globe. India, with its rapidly expanding digital ecosystem, is increasingly relying on AI-driven applications for public administration, law enforcement, healthcare, transportation, and financial services. Despite this exponential growth, the legal and regulatory architecture governing AI remains fragmented, relying primarily on sector-specific laws, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and various policy documents. This paper critically examines the adequacy of existing legal frameworks in addressing the unique ethical, legal, and socio-technical challenges posed by AI. The analysis begins with an overview of current Indian laws applicable to AI, evaluating gaps pertaining to accountability, algorithmic transparency, data governance, and cyber-security. Special attention is given to the Information Technology Act, 2000 (IT Act) and its provisions relating to electronic contracts, intermediary liability, due diligence obligations, and cybercrimes involving AI systems. The Digital Personal Data Protection Act, 2023 (DPDPA) is analysed for its principles of lawful processing, consent requirements, duties of Data Fiduciaries, and rights of Data Principals in the context of AI training datasets and automated decision-making.

Recognising limitations within the prevailing legal regime, the paper argues for a dedicated AI law that is adaptive, risk-based, and future-ready. Drawing comparative insights from the European Union's AI Act—featuring unacceptable, high, limited, and minimal-risk classifications—and the United States' evolving policy landscape driven by executive orders and voluntary frameworks, the paper evaluates different regulatory philosophies. Furthermore, it explores crucial themes such as cross-border data flows, data sovereignty, jurisdictional complexities, and India's strategic stance in securing digital autonomy.

The study also examines India's role in international collaborations on AI governance through institutions such as UNESCO, OECD, and G20, especially in standard-setting, ethical guidelines, and global frameworks on autonomous weapon systems (AWS). Issues of liability, accountability, and responsibility in AI decision-making are analysed within the domains of torts, contracts, product liability, autonomous vehicles, and medical diagnostics. The paper underscores the importance of human oversight in AI systems, highlighting the concepts of meaningful human control, human-in-the-loop, and human-on-the-loop frameworks. Ethical concerns surrounding transparency, explainability, algorithmic bias, discrimination, and fairness are evaluated through emerging global FAT (Fairness, Accountability, Transparency) principles.

Finally, practical aspects of AI legal education—such as moot courts, simulations, experiential learning, film reviews, news analyses, and field visits—are proposed to strengthen professional competence in AI law. Conclusively, the paper advocates for a comprehensive, multi-layered, and ethically informed AI legal ecosystem that aligns with international best practices while safeguarding India's socio-legal realities and technological aspirations.

Keywords: Artificial intelligence law, AI regulation India, it Act 2000, Digital Personal Data Protection Act 2023, intermediary liability, data sovereignty, EU AI Act, US AI Policy, algorithmic bias, explainability, AI accountability, meaningful human control, autonomous systems, tort liability, product liability, digital governance, cross-border data flow, ethical AI, Fat Principles, AI governance

Introduction

Artificial Intelligence (AI) is increasingly reshaping socio-technical systems across the world, influencing economic decision-making, public administration, policing, healthcare diagnostics, financial transactions, and interpersonal communication. India, with its massive population, rapidly expanding digital infrastructure, and ambitious Digital India initiative, has emerged as one of the world's largest markets and testing grounds for AI-powered solutions. From face recognition tools deployed by law enforcement to algorithmic lending platforms, predictive policing applications, agricultural advisory systems, and smart mobility solutions, AI is becoming deeply embedded in governance and everyday life.

However, this rapid deployment of AI raises significant concerns relating to privacy, autonomy, algorithmic discrimination, unexplained decision-making, cyber-security vulnerabilities, opacity in governance, and unclear liability frameworks. Existing Indian laws—primarily the Information Technology Act, 2000 and sectoral regulations—were not enacted with AI in mind. While they partially extend to AI activities, they fall short in addressing unique challenges such as model training on personal datasets, deepfake generation, autonomous decision-making, and the accountability vacuum created when AI systems operate beyond direct human oversight. Recent developments—including the Digital Personal Data Protection Act, 2023 (DPDPA), National Strategy for AI (NITI Aayog), the Responsible AI principles, and broad frameworks for digital governance—indicate India's evolving approach. However, the absence of a dedicated AI legislation continues to generate ambiguities, especially when compared to the European Union's AI Act and the United States' flexible, innovation-driven approach. This

paper aims to critically analyse the current legal landscape governing AI in India, highlight gaps, and propose pathways toward a comprehensive, future-ready, ethical AI law.

Existing Frameworks Regulating AI in India

Though India does not yet have a single, consolidated AI law, multiple statutes and policies indirectly regulate AI systems. These include

1. Information Technology Act, 2000 and rules
2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
3. Digital Personal Data Protection Act, 2023
4. Indian Penal Code, 1860 and Bharatiya Nyaya Sanhita, 2023
5. Sector-based regulations (RBI guidelines, IRDAI rules, medical device law, transport law, etc.)
6. Competition Act, 2002
7. Consumer Protection Act, 2019
8. Copyright Act, 1957
9. NITI Aayog's Responsible AI Framework

1. Sector-Specific Laws Affecting AI

AI systems operate across domains, so regulatory obligations differ

a. Healthcare and Medical Diagnostics

AI-driven diagnostic tools, predictive models, and robotic surgery systems raise issues of

1. medical negligence
2. informed consent
3. accuracy of automated diagnosis
4. liability of hospitals vs. developers

Medical Device Rules, 2017 regulate software intended for diagnosis or treatment, yet do not define AI or adaptive algorithms clearly.

b. Financial Sector

AI-based credit scoring, algorithmic lending and fraud detection are governed by

1. RBI's Fair Practices Code
2. RBI Guidelines on Digital Lending, 2022
3. Anti-money laundering rules

Concerns include opaque automated credit denials and discriminatory scoring.

c. Law Enforcement

AI-enabled

1. facial recognition
2. predictive policing
3. automated surveillance

have significant implications for privacy and misuse, with no dedicated statutory safeguards.

2. General Legal Gaps in AI Governance

Across sectors, the same challenges persist

1. No legal definition of AI
2. No risk classification framework
3. No clarity on liability for autonomous decisions
4. No mandatory explainability standards
5. No audit or bias-testing requirements
6. No governance framework for large language models (LLMs)
7. Weak safeguards against deepfakes
8. Limited cyber-security obligations for AI developers
9. No regulation for automated decision-making in public sector use

India's legal system thus addresses AI indirectly—creating ambiguities and inconsistencies.

Information Technology Act, 2000 and AI Governance

The IT Act, 2000 remains India's central digital law. However, it predates modern AI systems. Yet many of its provisions still apply to AI activities, either directly or by extension.

1. Application of the IT Act to AI-Generated Digital Contracts and Electronic Records

Section 4–10 of the Act recognise

1. electronic signatures
2. electronic records
3. digital contracts

AI-generated or AI-negotiated contracts raise questions

1. Can an AI agent form valid consent?
2. Who is the contracting party—the user or the developer?
3. Can algorithmic contracts be void for lack of "free consent" under the Indian Contract Act, 1872?

Courts have not yet interpreted these questions, causing legal uncertainty.

2. Intermediary Liability and Due Diligence Rules for AI Platforms

Under Section 79 of the IT Act and the 2021 Rules

1. platforms hosting AI content (e.g., deepfakes, AI art, chatbot outputs) are considered intermediaries
2. they must exercise due diligence
3. they can lose "safe harbour protection" if they do not act on harmful content

AI platforms must

1. prevent misuse
2. remove harmful outputs
3. label manipulated content
4. maintain user records

Yet, the 2021 Rules were drafted for social media—not for generative AI—leaving interpretive gaps about LLMs and autonomous systems.

3. Cyber-Security and Cybercrimes Involving AI

AI enables sophisticated cyber offences

1. deepfake blackmail
2. automated phishing through AI voice cloning
3. AI-assisted hacking
4. malware that learns and evolves

The IT Act criminalises

1. unauthorised access
2. computer manipulation
3. identity theft

4. cyber fraud

BUT does not address
1. autonomous cyber-attacks
2. AI-generated cyber weapons
3. liability when AI acts without direct human intent

Thus, India lacks cyber-security standards for AI developers, posing significant national security risks.

Digital Personal Data Protection Act, 2023 (DPDPA) and AI Regulation

The DPDPA is India's landmark privacy law. AI systems—particularly machine learning models—depend heavily on data processing. The Act introduces
1. principles of lawful processing
2. purpose limitation
3. consent requirements
4. data fiduciary obligations
5. rights of data principals

1. Lawful Processing and Consent for AI Training Data

AI models require
1. massive datasets
2. continuous data updates
3. real-time personal information

The DPDPA mandates
1. consent-based processing
2. notice requirements
3. purpose limitation
4. minimal data collection

For AI, this raises practical challenges
1. How to obtain consent for training datasets scraped from the internet?
2. Can broad consent be used for model training?
3. Should users have the right to withdraw data used in trained models?

The Act does not explicitly address automated decision-making or profiling—creating interpretive ambiguities.

2. Obligations of Data Fiduciaries in AI Context

Data Fiduciaries must
1. ensure transparency
2. maintain accountability
3. implement safeguards
4. prevent discrimination
5. conduct risk assessments (especially for "significant data fiduciaries")

For AI developers, this means
1. documenting training datasets
2. ensuring fairness
3. conducting algorithmic audits
4. enabling user explanations

However, none of these are explicitly codified for AI.

3. Rights of Data Principals in AI Decision-Making

DPDPA provides
1. right to access
2. right to correction
3. right to grievance redressal
4. right to nominate

Yet users may require additional rights
1. right to explanation for automated decisions
2. right to contest algorithmic profiling
3. right to be forgotten from AI training datasets

India's law does not yet provide these, unlike the EU GDPR.

Need for a Dedicated AI Legal Framework in India

While existing laws offer partial coverage, they do not address the technological and ethical complexities of modern AI systems. The lack of a unified AI statute results in regulatory fragmentation, inconsistent interpretations across sectors, and limited protection for citizens affected by automated decisions.

1. Arguments for a Holistic and Future-Proof AI Law

A dedicated AI regulation would allow India to

a. Establish a legally-binding definition of AI

India currently has no statutory definition of
1. Artificial Intelligence
2. Autonomous systems
3. High-risk AI
4. AI-driven decision-making

A law could adopt a tiered and technology-neutral definition similar to the EU AI Act.

b. Create risk-based classifications

Different AI uses involve different levels of risk
1. Minimal risk (spam filters, AI translation tools)
2. Limited risk (chatbots, recommendation systems)
3. High risk (healthcare diagnostics, financial scoring)
4. Unacceptable risk (mass surveillance, social scoring, biometric profiling without safeguards)

India currently treats all AI systems uniformly, which is ineffective.

c. Establish clear accountability

AI poses complex questions
1. Who is responsible when AI makes a mistake?
2. Can developers be sued for AI malfunction?
3. Should autonomous AI have "electronic personhood"?
4. Should liability shift depending on the level of autonomy?

A law is necessary to allocate responsibility clearly among
1. developers
2. deployers
3. users
4. manufacturers
5. data fiduciaries

d. Ensure algorithmic transparency and explainability

AI outputs can be
1. opaque
2. non-explainable

3. non-auditable

India currently has no statutory requirement for:
1. Bias audits
2. Algorithmic audits
3. Explainability reports
4. transparency obligations

e. Address ethical issues: bias, discrimination, autonomy

Examples include
1. discriminatory credit approvals
2. racially biased facial recognition
3. caste-based bias in automated hiring
4. gendered outcomes in health diagnostics

Without a law, citizens lack remedies.

f. Regulate military and autonomous weapon systems (AWS)

India has no framework addressing
1. AI-based surveillance drones
2. autonomous weapons
3. AI-enabled targeting systems

A dedicated law can create oversight mechanisms.

2. Addressing Accountability Gaps: Bias, Autonomy, and Explainability

AI systems create "responsibility vacuums" where
1. human hands are not directly involved
2. decisions occur without human intent
3. bias emerges from training datasets
4. explainability becomes computationally difficult

Thus, the law must include
1. mandatory bias testing
2. human-in-the-loop requirements
3. algorithmic impact assessments
4. safety and robustness standards
5. ethics committees for high-risk AI

Global AI Policy Comparison: India, European Union, and United States

To design a robust legal system, India must study global trends. The EU and US represent two distinct approaches to AI governance—prescriptive vs. voluntary.

1. European Union AI Act: A Risk-Based Model

The EU AI Act, passed in 2024, is the world's first comprehensive and legally binding AI regulation.

1.1. Classification of AI Systems by Risk

a. Unacceptable Risk – Completely Prohibited

Includes
1. social scoring by governments
2. real-time biometric identification in public (with exceptions)
3. subliminal manipulation techniques
4. AI that exploits vulnerable groups

These are banned because they threaten fundamental rights.

b. High-Risk AI Systems – Strictly Regulated

Includes
1. medical diagnostic AI
2. credit scoring models
3. biometric identification
4. AI in employment and exams
5. AI used in law enforcement
6. AI used in migration and border control

Requirements include
1. conformity assessment
2. documentation and logging
3. transparency
4. cyber-security standards
5. human oversight
6. comprehensive audits

c. Limited Risk – Transparency Requirements

Includes
1. chatbots
2. generative AI models
3. deepfakes

Users must be informed they are interacting with AI.

d. Minimal Risk – No Restrictions

Includes
1. AI video games
2. spam detection systems

1.2. Generative AI Regulation in EU

For models like ChatGPT or Gemini, obligations include
1. publishing training dataset summaries
2. ensuring copyright compliance
3. preventing harmful or illegal content
4. watermarking deepfakes
5. conducting risk mitigation assessments

1.3. Relevance for India

India could adopt
1. mandatory risk-based classification
2. audit requirements for high-risk systems
3. transparency for chatbots
4. watermarking and deepfake detection rules
5. prohibitions on harmful AI practices

2. United States Approach: Decentralized and Innovation-Friendly

The U.S. uses a sector-based, voluntary approach, driven by
1. Executive Orders (2023, 2024) on AI Safety
2. NIST AI Risk Management Framework (RMF)
3. State-level AI laws (California, Colorado, New York)
4. FTC (Federal Trade Commission) enforcement

2.1. Characteristics of the U.S. Model

a. No single AI laws

Instead, multiple agencies regulate AI within their domain
1. FDA → AI in medical devices
2. FTC → algorithmic fairness
3. DOT → autonomous vehicles
4. DOD → autonomous weapons

b. Voluntary AI ethics principles
E.g., transparency, fairness, accountability—non-binding.

c. Strong focus on innovation
The US avoids strict regulation that may slow technological growth.

d. Emphasis on national security
Large focus on
1. AI-enabled cyber defense
2. AI in military systems
3. research funding for safe AI

2.2. Lessons for India
India may adopt
1. flexibility and innovation-first approach
2. sectoral oversight
3. a national AI safety authority
4. adaptive regulation for emerging models
5. standards for testing large models

3. Comparative Evaluation: Prescriptive vs. Voluntary Models

Feature	EU Model	US Model	India (Current)
1. Nature	Prescriptive, binding	Voluntary, flexible	Fragmented
2. Risk Classification	Yes	No	No
3. Generative AI Rules	Strong	Limited	None
4. AI Rights for Citizens	Strong	Moderate	Weak
5. Enforcement Agency	Central AI Authority	Sectoral Agencies	None
6. Liability Framework	Clear	Evolving	Absent
7. Ethics Requirements	Mandatory	Optional	Policy-level only

India's future law can combine the best of both
1. EU's strong rights and risk categorization
2. US's innovation-friendly flexibility

Cross-Border Data Flow and Digital Sovereignty in AI
India's digital ecosystem depends heavily on global data flows. However, AI training requires massive datasets, and global AI companies rely on cross-border data transfer.

1. Legal Implications of Data Localization
India has debated data localization through
1. Draft Personal Data Protection Bills (2019, 2021)
2. RBI rules for payments data
3. CERT-In logging requirements

The 2023 DPDPA relaxes earlier strict localization demands but still allows
1. government restrictions on sensitive data export
2. national security-based controls
3. consent-based data transfer

Implications for AI
1. LLMs trained on Indian user data stored abroad raise privacy risks
2. foreign AI systems may not comply with Indian safety standards
3. absence of localization could hinder law enforcement
4. over-restrictive localization could harm innovation

A balanced approach is needed.

2. Jurisdiction and Enforcement Challenges in Global AI Models
AI companies often
1. host data on foreign servers
2. train models using global datasets
3. deploy services via cloud computing

This creates challenges
a. Whose law applies when AI harms Indian citizens?
Example: A foreign AI credit scoring tool denies an Indian applicant.
b. How can Indian courts enforce orders on foreign AI firms?
c. How can regulators audit models stored outside India?
d. How to ensure accountability when AI is trained on transnational datasets?

India requires cross-border enforcement mechanisms and mutual cooperation agreements.

3. Concepts of Digital Sovereignty and AI Autonomy
Digital sovereignty refers to a nation's ability to control:
1. data
2. digital infrastructure
3. AI ecosystems
4. cybersecurity
5. digital public platforms

For India, this includes
1. independent AI models (IndiaAI Mission)
2. secure digital public infrastructure (DPI)
3. national AI safety standards
4. control over critical infrastructure (banking, telecom, military systems)
5. avoiding overdependence on foreign AI technologies

AI sovereignty is becoming essential for
1. national security
2. economic competitiveness
3. technological autonomy

International Collaborations on AI Governance
AI governance requires global cooperation because AI systems do not obey borders.

1. Role of Global Organizations: UNESCO, OECD, G20
a. UNESCO Recommendation on AI Ethics (2021)
Focus on
1. human rights
2. transparency
3. environmental sustainability
4. fairness
5. gender equality

India supports and applies UNESCO principles in policy documents.

b. OECD AI Principles

These principles form the basis of the G20 AI Guiding Principles

1. Transparency
2. Robustness
3. Security
4. Accountability
5. human-centric design

c. G20 Digital Economy Working Group (DEWG)

India, during its G20 Presidency (2023) [13], emphasized

1. responsible AI
2. open-source digital public infrastructure
3. cross-border data governance
4. AI for social good

2. International Agreements and Standardization of AI Safety

Global attempts to harmonize safety standards include

1. EU–US Trade and Technology Council (TTC)
2. GPAI (Global Partnership on AI)
3. Standards by ISO, IEC, and IEEE
4. UN discussions on autonomous weapons

These frameworks support

1. common AI risk definitions
2. shared testing protocols
3. global safety benchmarks
4. cooperation on cyber-security

India actively participates in GPAI to strengthen its AI governance capacity.

3. Diplomacy and Regulation of Autonomous Weapons Systems (AWS)

AWS, including

1. autonomous drones
2. robotic weapons
3. AI-enabled targeting
4. lethal autonomous weapons (LAWS)

pose global ethical risks.

Key debates include

1. Should machines be allowed to decide life or death?
2. Is human control necessary?
3. How to assign liability for wrongful killings?

India's position

1. supports UN discussions
2. supports non-binding norms
3. has not endorsed a global ban
4. is developing indigenous military AI

A dedicated AI law could establish

1. clear human oversight in defense
2. rules for deployment
3. accountability mechanisms

Liability, Accountability, and Responsibility in AI Decision-Making

Artificial Intelligence challenges traditional legal concepts of liability because decisions are increasingly automated, opaque, or autonomous. Determining responsibility in AI-related harm requires an understanding of technology, human involvement, and legal principles.

Liability can arise in sectors such as

1. autonomous vehicles
2. AI-based medical diagnosis
3. algorithmic credit scoring
4. automated hiring systems
5. robotic surgeries
6. predictive policing

1. Determining Liability for AI Decisions

1.1. Traditional Legal Frameworks: Torts, Contracts, and Product Liability

The following doctrines apply to AI-induced harm

a. Tort Law

Liability may arise through

1. Negligence
2. strict liability
3. vicarious liability

Challenges arise when

1. AI acts without human instruction
2. harm is caused by algorithmic bias
3. AI predictions malfunction

Key tort questions include

1. Who is the "reasonable person" in AI negligence?
2. What constitutes foreseeability when AI is self-learning?
3. Can developers foresee all risks in AI behaviour?

b. Contract Law

Contracts using AI may face

1. errors in algorithmic communication
2. breach caused by automated systems
3. unconscionable terms generated by AI
4. click-wrap agreements processed by chatbots

AI may act as an "agent," but lacks legal personhood.

c. Product Liability

AI can be treated as

1. a product
2. a service
3. a hybrid system

Developers may face

1. manufacturing defect claims
2. design defect claims
3. failure to warn liability

Self-learning systems complicate accountability because they evolve beyond design.

2. Liability Shifting: From User & Developer to AI

Some scholars propose the concept of "electronic personhood" for autonomous AI systems.

Arguments for legal personhood

1. AI makes decisions independently
2. AI adapts beyond human intention
3. AI may act unpredictably

Arguments against

1. AI lacks consciousness
2. AI cannot bear punishment

3. AI cannot pay compensation
4. It may shield developers from liability

India must avoid creating a personhood loophole, ensuring
1. humans remain accountable
2. developers cannot escape responsibility
3. deployers maintain oversight

3. Sector-Specific Liability Issues

a. Autonomous Vehicles

Questions include
1. Who is liable in an accident?
2. The driver?
3. The manufacturer?
4. The software developer?
5. The sensor provider?
6. The AI algorithm itself?

A hybrid liability model is needed
1. Manufacturer responsible for design defects
2. Developer responsible for algorithmic faults
3. Owner responsible for maintenance
4. Government responsible for standards and infrastructure

b. AI in Medical Diagnostics

AI tools assist in
1. Radiology
2. Pathology
3. Cardiology
4. predictive risk assessment

Challenges
1. misdiagnosis by AI
2. overreliance by doctors
3. inadequate dataset diversity
4. lack of explainability

Potential liabilities
1. doctors → clinical negligence
2. hospitals → vicarious liability
3. developers → defective algorithm
4. regulators → inadequate oversight

India requires
1. certification of medical AI
2. post-market surveillance
3. audit trails
4. error reporting

Human Oversight in Autonomous AI Systems

While AI automates complex decisions, human oversight remains indispensable, especially for high-risk applications.

1. Meaningful Human Control (MHC)

MHC implies
1. Humans remain in charge
2. Humans can override AI
3. AI must remain predictable
4. Decision-making must be transparent
5. Accountability must be traceable

MHC is critical for
1. autonomous vehicles
2. predictive policing
3. drone surveillance
4. algorithmic justice systems
5. AI-assisted warfare

2. Human-in-the-Loop vs. Human-on-the-Loop

Human-in-the-Loop (HITL)

Humans actively supervise and approve decisions.

Used in
1. medical diagnostics
2. loan approvals
3. hiring decisions
4. military targeting

Human-on-the-Loop (HOTL)

Humans monitor and intervene only if needed.

Used in
1. semi-autonomous drones
2. automated traffic systems
3. industrial robotics

Human-out-of-the-Loop (HOOTL)

Fully autonomous systems with no human interaction.

Used in
1. high-frequency trading algorithms
2. some lethal autonomous weapons

India must regulate the use of HOOTL systems and restrict deployment in sensitive areas like law enforcement and military action.

3. Legal Implications of Human Non-Intervention

Non-intervention occurs when humans
1. blindly trust AI
2. fail to supervise
3. rely excessively on algorithmic outputs
4. lack technical knowledge

Legal consequences
1. negligence for failing to intervene
2. contributory liability
3. breach of statutory duties (e.g., doctors relying solely on AI)
4. enhancement of vicarious liability for institutions

Ethical Issues in AI-Driven Accountability

AI raises deep ethical concerns due to opaque decision-making, training dataset biases, and discriminatory outputs.

1. Transparency and Explainability (Right to Explanation)

Users affected by AI decisions may demand:
1. why the decision was made
2. what data influenced the output
3. how the algorithm works
4. whether bias affected the decision

Explainability challenges
1. deep learning models are black-box systems
2. AI decision pathways are non-linear
3. model complexity makes human explanation difficult

India currently lacks a "right to explanation," unlike the EU's GDPR and AI Act.

2. Algorithmic Bias and Discriminatory Outcomes

Bias sources

1. biased datasets
2. unrepresentative training samples
3. human prejudices encoded in data
4. proxy variables (caste, religion, gender)
5. skewed historical records

Examples affecting India

1. caste-based discrimination in automated hiring
2. gender bias in credit scoring
3. racial bias in facial recognition (skin tone errors)
4. discriminatory policing algorithms

India must mandate

1. bias testing
2. fairness metrics
3. periodic audits
4. transparency in datasets

3. Implementing FAT (Fairness, Accountability, Transparency) Principles

Fairness

AI must ensure

1. non-discriminatory outputs
2. representational equity
3. safeguards for vulnerable populations

Accountability

Stakeholders must be accountable for

1. data quality
2. algorithmic design
3. misuse
4. harm and losses
5. compliance with safety standards

Transparency

Developers and deployers must disclose

1. dataset origins
2. model logic
3. known risks
4. limitations
5. potential harms

India's forthcoming AI law should embed FAT into statutory requirements.

Practical Aspect: Legal Education and Experiential Learning in AI Governance

To prepare future lawyers, judges, police officers, policymakers, and scholars, practical tools and experiential learning help bridge the gap between theory and real-world implications.

1. Self-Learning Projects

Examples

1. coding simple machine learning models
2. analyzing ethical dilemmas in AI use
3. studying landmark AI court cases
4. researching bias in datasets

Such projects enhance technical literacy.

2. Presentations and Seminars

Students can present on

1. EU AI Act
2. AI in criminal justice
3. Deepfake regulation
4. Cross-border data flow
5. Algorithmic transparency

This builds analytical and communication skills.

3. Moot Courts and Legal Simulations

AI-specific moot problems may include

1. wrongful arrest based on facial recognition
2. liability for autonomous vehicle accidents
3. discrimination in AI hiring
4. AI medical misdiagnosis
5. cybercrime by autonomous AI systems

Simulations teach advocacy, argumentation, and judicial reasoning.

4. Film Reviews, News Analysis, and Case Studies

Film review examples

1. The Imitation Game (AI history)
2. Ex Machina (AI ethics)
3. Her (human-AI interaction)
4. The Social Dilemma (algorithmic influence)

Students learn ethical, philosophical, and legal implications.

News review examples

1. deepfake scandals in elections
2. AI errors in Indian policing
3. judicial remarks on AI evidence
4. global AI policy developments

5. Field Visits and Guest Lectures

Field visits to

1. AI research labs
2. forensic science departments
3. cyber police stations
4. data centers
5. robotics labs

Guest lectures by

1. AI scientists
2. Policymakers
3. legal experts
4. data protection officers
5. cyber-forensics professionals

These broaden understanding of practical challenges.

Conclusion

Artificial Intelligence promises unprecedented advancements in governance, public administration, healthcare, finance, and education. However, these benefits come with ethical dilemmas, accountability challenges, and risks to privacy, security, and fundamental rights. India's current legal framework—rooted in the IT Act, DPDPA, and sectoral regulations—offers partial but inadequate governance for modern AI systems.

The need for a comprehensive AI law is urgent. It must incorporate

1. risk-based classification
2. mandatory transparency and fairness
3. algorithmic audits
4. strong data governance

5. cross-border enforcement mechanisms
6. accountability for developers and deployers
7. protection of citizen rights
8. oversight for autonomous systems
9. global best practices from EU and US models

AI's transformative power demands a regulatory framework that balances innovation with societal protection. With a forward-looking legal architecture grounded in ethics, technology-neutral principles, and practical enforceability, India can lead the world in responsible and human-centric AI governance.

References

1. Government of India. The Information Technology Act, 2000 (No. 21 of 2000). Government of India, 2000.
2. Government of India. The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Ministry of Electronics and Information Technology, 2023. MeitY+1
3. European Parliament, Council of the European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024. EUR-Lex+1
4. NITI Aayog. National strategy for artificial intelligence – #AIForAll. Government of India, 2018. NITI AAYOG+2M-Seva+2
5. UNESCO. Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization, 2021. UNESCO+2UNESCO+2
6. Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD, 2019. OECD Legal Instruments+2OECD Legal Instruments+2
7. Organisation for Economic Co-operation and Development. OECD AI principles. OECD, 2019. OECD AI+1
8. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce, 2023. NIST Publications+1
9. White House. Executive Order 14110: Safe, secure, and trustworthy development and use of artificial intelligence. The White House, 2023. Federal Register+1
10. Ministry of Electronics and Information Technology. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Government of India, 2021.
11. Reserve Bank of India. Guidelines on digital lending. Reserve Bank of India, 2022.
12. Telecom Regulatory Authority of India. Recommendations on data protection framework for India. TRAI, 2017.
13. G20. G20 New Delhi Leaders' Declaration (sections on digital public infrastructure and AI). Government of India (G20 Presidency), 2023.
14. Global Partnership on Artificial Intelligence (GPAI). GPAI working group reports on responsible AI. GPAI, 2022.
15. Press Information Bureau. DPDP Rules, 2025 notified [Press release], 2025. Press Information Bureau
16. Barfield W, Pagallo U. (Eds.). Research handbook on the law of artificial intelligence. Edward Elgar, 2018.
17. Crawford K. Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press, 2021.
18. Eubanks V. Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press, 2018.
19. Hildebrandt M. Smart technologies and the end of law: Novel entanglements of law and technology. Edward Elgar, 2015.
20. Kuner C. Transborder data flows and data privacy law. Oxford University Press, 2013.
21. Noble SU. Algorithms of oppression: How search engines reinforce racism. NYU Press, 2018.
22. O'Neil C. Weapons of math destruction: How big data increases inequality and threatens democracy. Crown, 2016.
23. Pasquale F. The black box society: The secret algorithms that control money and information. Harvard University Press, 2015.
24. Russell S, Norvig P. Artificial intelligence: A modern approach (4th ed.). Pearson, 2020.
25. Sandel MJ. What money can't buy: The moral limits of markets. Farrar, Straus and Giroux, 2012.
26. Solove DJ. Privacy law: Principles, laws, and practices (2nd ed.). Aspen Publishers, 2021.
27. Zarsky T. Information privacy in the digital age. Routledge, 2016.
28. Zuboff S. The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs, 2019.
29. Balkin JM. The free speech century and algorithmic governance (collected essays). Harvard University Press, 2020.
30. Susskind R. Online courts and the future of justice. Oxford University Press, 2019.
31. Narayanan A, Vallor S. (Eds.). Ethics of artificial intelligence. Oxford University Press, 2022.
32. Burrell J. How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 2016, 3(1).
33. Coglianese C, Lehr D. Regulating by robot: Administrative decision making in the machine-learning era. Georgetown Law Journal, 2017, 105.
34. Citron DK, Pasquale F. The scored society: Due process for automated predictions. Washington Law Review, 2014, 89.
35. Edwards L, Veale M. Slave to the algorithm? Why a right to an explanation is probably not the remedy you are looking for. Duke Law & Technology Review, 2017, 16.
36. Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, *et al*. AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 2018, 28.
37. Kroll JA, Huey J, Barocas S, Felten E, Reidenberg J, Robinson D, *et al*. Accountable algorithms. University of Pennsylvania Law Review, 2017, 165.
38. Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L. The ethics of algorithms: Mapping the debate. Big Data & Society, 2016, 3(2).
39. Selbst AD. Disparate impact in big data policing. Georgia Law Review, 2018, 52.

40. Selbst AD, Barocas S. The intuitive appeal of explainable machines. Fordham Law Review, 2018, 87.
41. Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 2017, 7(2).
42. Yeung K. Recommendation of the Council on Artificial Intelligence (OECD) – Commentary. International Legal Materials, 2020, 59(1). Cambridge University Press & Assessment
43. Veale M, Edwards L. Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. Computer Law & Security Review, 2018, 34(2).
44. Gasser U, Almeida V. A layered model for AI governance. IEEE Internet Computing, 2017, 21(6).
45. Green B, Viljoen S. Algorithmic realism: Expanding the boundaries of algorithmic thought. Fordham Law Review, 2020, 89.
46. Kuner C. Data protection, privacy and security in EU law. International and Comparative Law Quarterly, 2017, 66(3).
47. Balkin JM. Information fiduciaries and the First Amendment. UC Davis Law Review, 2015, 49.
48. Kaminski ME. The right to explanation, explained. Berkeley Technology Law Journal, 2019, 34.
49. Madan M, Sengupta A. Regulating artificial intelligence in India: Between innovation and rights protection. Indian Journal of Law and Technology, 2022, 18.
50. Saxena R, Chawla A. Algorithmic governance, data protection, and AI in India: A critical assessment of emerging frameworks. NUJS Law Review, 2021, 14.