# ARTIFICIAL INTELLIGENCE, ETHICS, AND LAW IN GOVERNANCE: STRIKING A BALANCE BETWEEN INNOVATION AND ACCOUNTABILITY

Shreya S, Sastra Deemed University, Thanjavur

**ABSTRACT**

Artificial Intelligence (AI) has become one of the most revolutionary forces changing governance, legal frameworks, and societal structures in the twenty-first century. Though its ability to improve administrative effectiveness, predictive administration, and legal judgment is vast, it also poses major ethical, legal, and constitutional challenges. This article embarks on an interdisciplinary analysis of the governance of AI by seeking to bridge the law, technology, and society viewpoints. It delves into the legal responsibility of AI decision-making, accountability in healthcare and administrative settings, data privacy and protection issues, algorithmic prejudice, and the balance between regulatory and innovation. Through close examination of statutes like the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and foreign instruments like the GDPR, the paper analyses how rules of law seek to balance technological upsets with constitutional rights. Indian and comparative case laws explain the shifting judicial response to AI accountability and fairness in algorithms. Also, the research questions whether the prevailing doctrines such as tort liability, constitutional protection, and human rights norms are sufficient or new regulatory models are needed. Through doctrinal and ethical research, the research reflects on the urgent need for a strong, transparent, and participatory governance regime for AI in India and the world.

## 1. Introduction

The emergence of Artificial Intelligence (AI) has transformed governance systems globally. Governments increasingly use AI systems to enhance the efficiency of public administration, judicial decisions, regulation of healthcare, welfare allocation, and security management. In India, AI is increasingly entering governance in the form of e-courts, predictive policing software, automatic welfare targeting, and biometric identification under Aadhaar. While such technologies promise efficiency, transparency, and scalability, they also pose basic questions of legality, ethics, and social justice. The real issue, thus, is not whether AI needs to be inserted into governance, but how law and institutions of regulation need to handle its deployment so that it fosters innovation while securing accountability and rights.

India's statutory landscape is still fractured and ill-suited to address the singular concerns of AI. The Information Technology Act, 2000 (IT Act) continues to be the prevailing statute governing online transactions, but its provisions were drafted in a bygone era of cybercrimes and e-commerce, not algorithmic control. For example, Section 66A, declared unconstitutional , demonstrated how open-ended provisions might abuse to limit online speech. Even though it was struck down, its continued invocation on the ground indicates the risks involved in invoking outdated statutory tools on new technological spaces[1]. Likewise, Section 69, enabling interception and surveillance of communications, coupled with AI-enabled surveillance tools such as facial recognition or predictive policing, presents disproportionate intrusions into the constitutional right to privacy[2]. Further, Section 69A, the legislation behind executive orders blocking online platforms, demonstrates how inscrutable state practices might get amplified if automated systems are making such choices without transparency or judicial scrutiny.

The Digital Personal Data Protection Act, 2023 (DPDP Act) has closed some of the legislative lacuna by acknowledging rights of data principals and placing obligations on data fiduciaries. However, in creating avenues for consent and institutional oversight in the form of the Data Protection Board, it ignores algorithmic obscurity, discriminatory judgments, or automatic profiling—issues at the centre of AI regulation. Without requirements of explainability, auditability, or fairness in algorithmic systems, people are left exposed to unfair or opaque state judgments. Therefore, although India has set in motion regulation of personal data, its regime

[1] Shreya Singhal v. Union of India (2015)
[2] K.S. Puttaswamy v. Union of India (2017)

is short in tackling the particular issues of AI in governance.

Policy interventions have attempted to bridge such gaps. The National Strategy for Artificial Intelligence of the NITI Aayog (2018) articulated the vision of an "AI for All," and the Principles for Responsible AI (2021) and their Operational Framework (2021) set out guidelines on fairness, accountability, and inclusivity. These are India's recognition of the imperative that the legal framework must be rooted in ethical principles. But being the soft-law instruments they are, they do not have binding effect, and hence, are non-enforceable and cannot, in themselves, assure compliance in such sensitive domains as policing, welfare dispensation, or judicial discretion.

The judiciary has also begun to address AI regulation. The Delhi High Court ordered the government to establish an Advisory Group on AI Regulation comprising representatives from the Ministry of Electronics and Information Technology, NITI Aayog, and the private sector to prepare techno-legal guidelines on AI[3]. Supreme Court petitions called for mandatory watermarking of AI-generated content, standalone algorithmic audit by CERT-In-empanelled entities, and creation of a National AI Regulation Authority under the IT Act to deal with existential threats to national security through deep fakes and election disinformation[4]. Such cases depict how Indian courts are attempting to make up for legislative lethargy, yet judicial interventions are piecemeal and response-oriented, not holistic.

Comparative experience offers hope as well as cautionary lessons. The European Union's Artificial Intelligence Act (2024) has been a trailblazer in developing a risk-based regulatory approach, setting strict requirements on high-risk systems such as those used in governance and public administration. The United States has developed softer solutions through its Blueprint for an AI Bill of Rights (2022) and Federal Trade Commission guidelines, emphasizing fairness and consumer protection. China's Social Credit System offers the risk of AI-facilitated authoritarian control, whereby machine decision-making directly impacts citizens' rights and freedoms. International norms such as the OECD Principles on AI (2019) and UNESCO's Recommendation on the Ethics of AI (2021) emphasize transparency, accountability, and human-centred design, setting normative standards for states, including India.

[3] Chaitanya Rohilla v. Union of India (2024)
[4] Narendra Kumar Goswami v. Union of India (2025)

It is against this global and Indian context that the research of the day positions itself. The central question is how exactly AI is being deployed in governance systems, at the global level and in India, and whether existing legal systems can keep up with the risks associated with it. The research also raises the legal, ethical, and societal concerns that emerge when governance decisions are intermediated by black-box algorithms, giving rise to concerns of bias, privacy, surveillance, and exclusion of marginalized groups. Most of all, it questions how legal systems—India's among them—can reconcile the promotion of technological innovation with accountability, transparency, and respect for constitutional rights. Through doctrinal analysis of legislation, judicial decisions, and policy proposals to comparative international models, this study contends that India needs a comprehensive AI law now. This law has to go beyond ad hoc statutory rules and voluntary ethics codes, and instead create a categorical system of accountability, open oversight mechanisms, and rights-based guarantees. In so doing, it has to balance the promise of innovation with the need for accountability, and thus ensure that AI governance supports and does not subvert the democratic and constitutional order.

## 2. Conceptual Framework of AI and Governance

AI has to be conceptualized in governance through a syncretic knowledge of technology, law, and ethics. Governance has in the past developed successively with technological revolutions printing, telecommunications, and the internet—each of which posed new regulatory issues. AI is the next frontier, and it has the potential to revolutionize state–citizen relations by facilitating predictive decision-making, automated service, and sophisticated analysis of data. But this evolution demands greater scrutiny of how AI is characterized, how governance is evolving in the digital age, and how legal frameworks need to respond to align innovation with accountability.

### 2.1 Defining and Characterising Artificial Intelligence

AI is itself a contested definition, which makes regulation more difficult. Broadly, AI is a description for computer systems that can accomplish high-level tasks requiring human intelligence, including pattern recognition, decision-making, and problem-solving. The EU's AI Act (2024) characterizes AI as "machine-based systems with varying degrees of autonomy, that can produce outputs like predictions, recommendations, or decisions that affect physical or virtual worlds." This definition by function is important for regulation because it encompasses both autonomous systems and decision-support tools employed by public

authorities.

In India, while no law clearly defines AI, policy papers like NITI Aayog's National Strategy for AI (2018) take a pragmatic turn, characterizing AI as an engine of socio-economic growth with the vision of "AI for All." This vision emphasizes inclusiveness, but its lack in binding legislation leaves a regulatory void. In legal language, AI has been obliquely mentioned in cases in which the Supreme Court discussed the dangers of deepfakes and algorithmic disinformation, silently acknowledging AI as a governance technology capable of disruptive transformation that needs to be regulated[5]. The lack of a statutory definition in India is to be contrasted with jurisdictions such as the EU, in which clear definitional limits are found to be necessary for effective risk stratification and allocation of liability.

### 2.2 The Evolution of Governance in the Digital Age

Digital-era governance is no longer solely a function of human discretion and bureaucratic choice, but one that increasingly depends on algorithmic mediation. For instance, India's Aadhaar scheme under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, uses biometric verification systems aided by algorithmic processes to decide entitlement to welfare schemes. The Supreme Court allowed Aadhaar while emphasizing proportionality and data protection measures, thus implicitly recognizing the dangers of automated governance[6]. In a parallel manner, the application of AI in policing in the form of facial recognition technology has evoked legal challenges, including legal action against the use of facial recognition by the Delhi Police during protest periods, reflecting the tensions between technological effectiveness and constitutional freedoms.

Internationally, AI in governance embodies varied trajectories. The EU places focus on a model centered around rights using tools such as the General Data Protection Regulation (GDPR, 2016) and the AI Act (2024). Conversely, China's Social Credit System is a state-led model, integrating AI within surveillance and behavioural scoring. The comparative models illustrate how paradigms of governance evolve differently: liberal democracies tend to be unable to reconcile rights with innovation, whereas authoritarian regimes tend to give preference to control at the state level. India being a constitutional democracy, it thus has to tread cautiously between gains in efficiency and its commitments to protect fundamental rights under Articles

[5] Narendra Kumar Goswami v. Union of India (2025)
[6] K.S. Puttaswamy (Aadhaar-5J) v. Union of India (2018)

14, 19, and 21 of the Constitution.

### 2.3 Law, Technology, and Governance: An Interdependent Triad

Law, technology, and governance are an interdependent triad where each shapes and informs the other. Technology brings new forms of governance tools, law gives normative structures for legitimacy, and governance realizes these into administrative frameworks. The IT Act, although not very effective in regulating AI, shows how law strives to keep up with technological evolution. The Delhi High Court's instructions to create an Advisory Group for AI Oversight reflect efforts to bring law into conformity with new technology realities[7].

Alongside, legal gaps pose crucial questions. Algorithmic decision-making, for example, tends to be opaque, and the constitutional promise of equality before law is called into question. And if two people are treated unequally by opaque algorithms, is this a breach of Article 14? Courts have not yet directly answered that question, but the reasoning of precedents, whereby arbitrariness was considered contrary to equality, would imply that arbitrary outcomes by algorithms could also invite constitutional challenge. This highlights the pressing necessity to locate AI not just as a technology, but as a governance actor subject to legal norms[8].

### 2.4 Interdisciplinary Foundations for AI Governance

AI governance must be understood through an interdisciplinary approach, combining understandings from law, ethics, sociology, and political science. Technological regulation alone is not enough, given that algorithmic systems incorporate inculcated human prejudices and socio-political environments. Ethical guidelines like UNESCO's Recommendation on the Ethics of AI (2021) and India's Principles for Responsible AI (2021) prioritize transparency, accountability, and fairness, but implementing these into workable legal standards proves to be a task.

Sociological criticisms point out that AI systems tend to replicate and exacerbate entrenched inequalities, especially when technology access is unequal. For instance, algorithm-driven welfare programs can leave behind marginalised groups who do not possess digital literacy or participate in identification systems. Likewise, predictive policing systems can

[7] Chaitanya Rohilla v. Union of India (2024)
[8] E.P. Royappa v. State of Tamil Nadu (1974)

disproportionately target vulnerable populations and perpetuate historical biases. These concerns necessitate the inclusion of not just doctrinal protections but also socio-ethical aspects within legal frameworks to facilitate inclusive governance.

### 2.5 Towards a Conceptual Framework

The conceptual framework of governance and AI therefore yields three linked insights. First, clarity of definition is paramount, since legislative vagueness prevents efficient regulation. Second, digital-age governance cannot be separated from the issue of rights, accountability, and fairness, especially considering India's constitutional commitments. Third, an interdisciplinary foundation is necessary, since law is incapable of grasping the dynamic interplay of technology and society. As such, the issue of how legal systems can balance support for innovation and the provision of accountability must be placed within this more general conceptual framework.

By charting the definitional boundaries of AI, tracing the development of digital-age governance, and positioning the law–technology–society intersection, the chapter lays the foundation for examining India's patchwork legal responses. It also places the research's wider objective: assessing whether current statutory regimes and judicial initiatives are sufficient, and if not, proposing a framework that brings together innovation with constitutional responsibility in AI-governance

## 3. Legal Frameworks for Regulating AI in Governance

It is a delicate task to regulate Artificial Intelligence (AI) in governance, where there is a need to balance stimulating innovation and stimulating accountability. In contrast to conventional technologies, AI introduces challenges of opacity, autonomy, and unpredictability that conventional legal frameworks are ill-equipped to meet. India has taken a patchy approach till date, depending on generic digital legislation and policy guidelines, whereas international jurisdictions have started outlining more specialised instruments. A comparative analysis of national and international regimes identifies both the lacunae and possibilities for India in building an integrated AI governance framework.

### 3.1 National Approaches: The Indian Context

India does not have a specific AI law, and regulation is currently based on general information

technology and data protection legislation. The Information Technology Act, 2000 (IT Act) continues to be the central legislation. Although it does not mention AI in particular, a number of provisions find application to algorithmic governance. Section 43A places liability on not keeping sensitive personal data secure, a provision which gains new meaning in the context of processing by AI systems massive data sets. Section 66 deals with hacking and misuse of data, applicable to intrusion involving AI systems. Section 69, which authorizes government officials to intercept, monitor, or decrypt electronic communications, has been used in surveillance situations, evoking sharp concern in conjunction with AI-based facial recognition and predictive policing.

Judicial oversight has to some extent shed light on these threats. The Supreme Court identified privacy as a right under Article 21, requiring proportionality and necessity by the state in surveillance[9]. This principle directly limits AI-facilitated governance, particularly where mass facial and biometric recognition systems are used. The Court nullified Section 66A of the IT Act, emphasizing the risks of imprecise statutory language that might open up the door to arbitrary curtailment of free expression[10]. These judgments emphasize that legal provisions, no matter how technology-agnostic, need to survive constitutional testing when used in relation to AI.

More recently, the Digital Personal Data Protection Act, 2023 (DPDP Act) provided a rights-based approach to personal data processing, such as duties of lawful purpose, data minimisation, and storage limitation. Although important, the Act does not impose obligations of algorithmic transparency, fairness, or accountability on automated decision-making, in contrast to the General Data Protection Regulation (GDPR) in the European Union. AI governance in India, therefore, is still only partially addressed under privacy regulation, without wider protections against algorithmic bias or liability.

### 3.2 United States: A Soft-Law Model

The United States has steered clear of blanket AI legislation, opting instead for sectoral and rights-focused approaches. The Blueprint for an AI Bill of Rights (2022), which the White House issued, sets out five principles: safe and effective systems, algorithmic discrimination protection, data privacy, notice and explanation, and human alternatives. Although non-

[9] K.S. Puttaswamy v. Union of India (2017)
[10] Shreya Singhal v. Union of India (2015)

binding, these principles have shaped federal and state policy. Moreover, the Federal Trade Commission (FTC) has used consumer protection and anti-discrimination laws to sanction unfair algorithmic conduct, demonstrating a reliance on existing regulation requirements.

In practice in the courts, cases like the debate over the COMPAS algorithm and sentencing (State v. Loomis, 2016, Wisconsin Supreme Court) raised due process issues when transparent algorithms shape court decisions. Although not precedential in India, these cases share the dangers of opaque algorithms in the administration of governments and affirm the importance of explainability in decision-making processes.

### 3.3 European Union: A Complete Statutory Framework

The European Union has led statutory regulation with the Artificial Intelligence Act (2024), the first-ever universal AI law in the world. The Act categorizes AI systems into four groups unacceptable risk, high risk, limited risk, and minimal risk and imposes rigorous duties on high-risk use cases, such as those in government, policing, migration, and judiciary. Requirements include transparency, human oversight, conformity assessments, and penalties for non-compliance. In addition to the GDPR (2016) limiting automated decision-making under Article 22, the EU regime has ensured AI in government is closely tied to rights-based protections.

To India, the EU model offers a template for ambitious statutory overhaul. It shows how risk-based regulation can balance innovation with accountability, underlining the need for increased vigilance over governance uses of AI. Critics, though, contend that high compliance costs could strangle smaller businesses, requiring India to dial such a model back to economic fact.

### 3.4 China: A State-Centric Approach

China offers an alternative model, integrating AI into state-centred governance structures. The Social Credit System, built on AI-facilitated surveillance and behavioural evaluation, exemplifies a model where technology is largely used for social control. The Measures for the Administration of Algorithmic Recommendation (2022), for example, places obligations upon providers but is largely geared toward maintaining state control rather than safeguarding individual rights. For India, then, this model is a warning: technologically aspirational, but raising basic questions regarding autonomy, privacy, and democratic control.

### 3.5 International Normative Frameworks

Outside of national regimes, international institutions have attempted to frame guiding principles. The OECD Principles on AI (2019) prioritise human rights, transparency, and responsibility, while the UNESCO Recommendation on the Ethics of AI (2021) focuses on inclusiveness, fairness, and sustainability. Even if not legally enforceable, these documents are part of an emerging global agreement that AI must be governed in a manner that prioritizes humanity and is rights-oriented. For India, which has adopted these principles, the test is in converting such soft-law obligations into enforceable statutory law.

### 3.6 Towards Legal Reform in India

The disorganized Indian system, contrasted with more systematic international examples, highlights the need for major reform. AI in the government invokes essential constitutional assurances of equality, freedom of speech, and privacy, but is still only regulated indirectly through non-binding policies and statutory provisions. Judicial intervention in Chaitanya Rohilla v. Union of India (2024) and Narendra Kumar Goswami v. Union of India (2025) reflect the judiciary's acknowledgment of potential risks, yet courts cannot replace legislative transparency.

Accordingly, India must move toward a dedicated AI statute, one that builds upon the IT Act and DPDP Act while addressing algorithmic bias, liability allocation, and transparency. Such legislation must incorporate comparative lessons from the EU’s rights-based statutory model, adapt soft-law guidance from the US and OECD, and consciously avoid the authoritarian risks exemplified by China. Only then can AI in governance be deployed in a manner that reconciles innovation with constitutional accountability.

## 4. Ethical Challenges in AI Governance

Governance with the help of Artificial Intelligence (AI) is not only difficult legally but also presents extremely basic ethical challenges. As compared to the classical problem of regulation, the ethics of AI present before us questions of justice, fairness, dignity, and autonomy that are beyond the legal domain. In India, where constitutional values support the system of governance, these challenges become even more urgent. The absence of detailed statutory provisions adds to reliance on ethical reasoning, applied with regard to comparative practices

and judicial insight. The chapter is concerned with the most important ethical concerns from AI in governance in the Indian constitutional order context, vis-à-vis the international experience.

### 4.1 The Problem of Algorithmic Bias and Discrimination

AI algorithms are no more fair than the data they have been trained on, but official data characteristically reproduces social inequalities and hierarchies. Algorithmic bias is then used to reinforce discrimination as a mask of neutrality. In India, this conflicts with constitutional safeguards under Article 14 (equality before the law) and Article 15 (non-discrimination). For example, AI facial recognition technologies applied in law enforcement have appeared globally to be at their finest in performing badly on minority groups, raising the risk of selective targeting.

Transnationally, the same risks were highlighted, wherein the Supreme Court of Wisconsin cautioned against the use of transparent AI algorithms during sentencing. Although the court permitted their use subject to exceptions, the ruling highlighted concerns for due process[11]. Algorithmic profiling could fall under similar scrutiny under, which extended the scope of Article 21 to require state action not to be arbitrary but to be just, fair, and reasonable. Application of discriminatory algorithms would likely fail the constitutional test[12]. The moral challenge is one of reconciling the efficiency of AI systems with the danger of injecting systemic prejudices into the machinery of the state.

### 4.2 Privacy, Autonomy, and Surveillance Issues

An equally pressing ethical issue is whether AI would undermine the autonomy of individuals with permanent surveillance. Aadhaar, ruled in K.S. Puttaswamy (Aadhaar-5J) (2018) with reservations, had already demonstrated the constitutional clash between state interests in efficiency and privacy and dignity rights of the individual. With AI, especially facial recognition, predictive policing, and online surveillance, the scale of intrusion increases.

Ethically, there is a breakdown of informed consent where citizens have little power over AI systems deployed by the state. This not only violates privacy pursuant to Article 21 but also

[11] State v. Loomis (2016)
[12] Maneka Gandhi v. Union of India (1978)

human dignity, which has been specifically identified by the Supreme Court[13]. Additionally, AI surveillance gives rise to autonomy concerns individuals may alter their conduct since they don't wish to be under constant surveillance, exerting a "chilling effect" similar to that has been presented in relation to restrictions on free speech[14].

Thus, the ethical problem is not so much that of legality as of whether systems of government should pursue efficiency at the cost of eroding essential conditions of human freedom.

### 4.3 Transparency and the "Black Box" Problem

A constitutional democracy's governance must be transparent and accountable. The majority of AI systems, however, are "black boxes" whose methods of decision making are too complex for human brains to understand. This creates extreme ethical challenges: if citizens do not understand how decisions were made, how can they object to them?

The EU's GDPR Article 22, which gives people the right not to be subjected to decisions by automated means that have legal effects without human intervention, is a normative response to this ethical problem. India's DPDP Act, 2023 has no such corresponding protection that leaves citizens vulnerable to secrecy in governance decisions.

Legally, the Supreme Court reiterated transparency as a constitutional principle in democratic governance through elections. Analogously, it can be argued that opaque algorithmic governance systems violate the same principle of responsible democracy. Ethically, the question is whether it is permissible to let the state hire out governance functions to systems whose underlying reasonableness remains closed to the impacted[15].

### 4.4 Accountability and the Question of Liability

AI architectures make it difficult for traditional accountability frameworks. If the damage is done by an AI-based decision in the government, say wrongful denial of a welfare benefit or illegal detention, then to whom can one attribute liability? The programmer, the agency deploying, or the state itself?

[13] Francis Coralie Mullin v. Administrator, Union Territory of Delhi (1981)
[14] Shreya Singhal v. Union of India (2015)
[15] Union of India v. Assn. for Democratic Reforms (2002)

Indian law has long accepted state liability for tortious actions under the doctrine of constitutional torts (Nilabati Behera v. State of Orissa, 1993). However, with AI, responsibility gets diffused and causation foggy. The ethical concern is whether or not accountability can be watered down just because the choice was mechanized. Comparative models, like the EU AI Act, place strict liability on deployers of high-risk AI systems, making sure that responsibility is not diverted. For India, then, such certainty is ethically necessary to prevent a governance regime in which harms get orphaned.

### 4.5 Human Dignity versus Technocratic Efficiency

AI is all about efficiency, speed, and objectivity, but administration is not merely about outputs—it is also about being courteous to citizens as rights-bearing individuals. The Supreme Court observed that even administrative orders have to satisfy the test of fairness and natural justice. Automated decision-making promotes dilution of this principle by putting individuals at the mercy of data points.[16]

This tension comes through most intensely in welfare governance. Withholding food rations due to Aadhaar-linked authentication failure, as technologically efficient as it is, has led to starvation fatalities, which poses the ethical concern: does technological efficiency trump human dignity and the right to life? Such moments illustrate how AI governance, if unregulated, has the potential to turn constitutional citizens into passive subjects of technocratic rule.

### 4.6 Democratic Legitimacy and Participation

Thirdly, AI poses ethical issues regarding democratic legitimacy. Algorithm-brokered governance decisions are most likely to evade public debate and supervision. Participatory ethical decision-making is characteristic of democracy, but algorithms localize authority among technical experts and state apparatuses remote from citizens' involvement.

Internationally, the UNESCO Recommendation concerning the Ethics of AI (2021) calls for inclusivity and participatory AI oversight. Domestically, this is in line with Article 19(1)(a) and Article 19(1)(c) protecting the right of the people to expression and association—prerequisites for participatory democracy. The ethical question then becomes whether AI regulation

[16] A.K. Kraipak v. Union of India (1969)

undermines democratic values through depersonalizing decision-making and removing it from citizen control.

### 4.7 Towards an Ethical Framework for India

India must move beyond compliance with the law to embrace an explicit ethical framework for AI in the government. This should involve norms of justice, accountability, transparency, and respect for human dignity, grounded in constitutional values. The Supreme Court's constitutional rights jurisprudence already has a normative anchor: non-arbitrariness (E.P. Royappa v. State of Tamil Nadu, 1974), privacy (Puttaswamy, 2017), and natural justice (Kraipak, 1969). By integrating these values into AI policy, India can ensure that technological progress does not come at the expense of ethics.

## 5. Societal Impacts of AI in Governance

The use of Artificial Intelligence (AI) in governance has deep societal implications that go beyond administrative convenience or efficiency. The incorporation of AI in public services, policing, justice administration, and healthcare reconfigures the social contract, impacting citizens' rights, opportunities, and belonging. As much as AI promotes better service delivery and predictive governance, it potentially intensifies inequalities, solidifies bias, and produces systemic exclusions. This chapter explores the social implications of AI rule-making in India and learns from global experiences to find opportunities and challenges.

### 5.1 AI in Justice Delivery

AI is gaining ground in judicial administration to accelerate case handling, analyze judicial precedents, and aid judicial decision-making. India's e-Courts Mission Mode Project and current AI pilots in case prediction and document analysis are examples of initiatives aimed at decreasing pendency. But the utilization of predictive AI systems is problematic regarding fairness, accountability, and transparency. The threat is that automated recommendations are regarded as authoritative, possibly influencing judicial thought without inquiry. Internationally, the COMPAS case (State v. Loomis, 2016) in the United States drew attention to how over-reliance on algorithmic risk assessment tools may result in racial discrimination in sentencing, threatening the foundations of due process and equality before the law.

In India, similar risks arise if AI software is blindly integrated into judicial processes. The

Supreme Court decided that arbitrariness was the opposite of equality, and therefore algorithmic choices must be examined for underlying bias[17]. Ethical use thereby demands transparency, human checks, and the facility for concerned parties to appeal algorithmic decisions so that AI supports justice, not just administrative convenience.

### 5.2 Healthcare Governance through AI

Healthcare governance, particularly in public health and welfare terms, increasingly uses AI for predictive analytics, disease surveillance, and allocation of resources. India's National Digital Health Mission (NDHM) foresees AI to improve diagnostics and personalize treatment. Such applications, however, raise liability and ethical issues. AI system errors leading to misdiagnosis or algorithmic errors that lead to inappropriate resource allocation could invoke civil and constitutional responsibility.

The DPDP Act, 2023, sets out some remedy for misuse of data but not for accountability for automated medical decision-making. Globally, ethical frameworks such as UNESCO's Recommendation on the Ethics of AI (2021) highlight fairness, explainability, and non-discrimination, promoting that algorithmic systems should augment but not displace professional judgment. As such, the social impact depends on striking a balance between gains in efficiency and accountability to ensure that AI in healthcare governance does not erode trust, equity, or human dignity.

### 5.3 AI in Policing and Security

AI use by law enforcement, such as predictive policing, facial recognition, and surveillance of crowds, has profound implications for civil rights. India has seen legal opposition to Delhi Police's facial recognition rollout, indicating possible breaches of privacy, freedom of expression, and freedom of assembly. The Supreme Court reiterated that mechanisms of surveillance need to satisfy proportionality and necessity tests, emphasizing that unregulated AI usage poses constitutional violations.[18]

Global experiences offer lessons of caution. In China, the Social Credit System illustrates how AI can be employed to track and shape citizen behaviour, with implications for autonomy and

[17] E.P. Royappa v. State of Tamil Nadu (1974)
[18] K.S. Puttaswamy v. Union of India (2017)

social stratification. The EU AI Act (2024) in contrast places strict requirements on high-risk AI systems in policing, such as human review and transparency requirements, to offer a rights-based framework for security governance.

### 5.4 Digital Divide and Exclusion of Marginalised Groups

AI governance risks reproducing existing social inequalities if access to technology is uneven. For example, algorithmic welfare distribution systems reliant on Aadhaar or biometric authentication can inadvertently exclude marginalized groups lacking digital literacy or documentation. Cases of food ration denial during the COVID-19 pandemic exemplify how technological governance, though efficient, can produce tangible harm.

Ethically, exclusion of this sort goes against Articles 14 and 21 of the Indian Constitution that assure equality and the right to life. Socially, it demeans faith in government, stripping digital interventions of legitimacy. Internationally, OECD principles prioritize inclusivity and equity, strengthening the case for developing AI systems with consideration for rich socio-economic contexts. Overcoming this challenge involves combining human-oriented AI frameworks, participatory design, and ongoing auditing to ensure that governance systems benefit all citizens in an equitable manner.

### 5.5 Intersections of Law, Ethics, and Society

The social consequences of AI in governance cannot be dissociated from ethical and legal implications. Machine decision-making, if unregulated, can selectively impact marginalized groups, perpetuate structural biases, and undermine transparency in bureaucratic processes. Judicial principles regarding equity, proportionality, and non-arbitrariness (Maneka Gandhi v. Union of India, 1978; E.P. Royappa, 1974) serve as normative touchstones in assessing AI effects, with international standards providing guidance on participatory, rights-based governance.

By integrating AI into governance, policymakers are challenged with the double requirement to realize technological potential and secure social justice. Designing, deploying, and auditing AI systems must thus be coordinated with constitutional protections, ethical considerations, and participatory governance techniques. Only with such integration can AI become a means of empowerment, not exclusion.

### 5.6 Towards Inclusive AI Governance

A forward-looking strategy necessitates not just legal adherence but preventive action to prevent harm to society. This involves setting up algorithmic audits, requiring impact assessments, and creating grievance redress mechanisms adapted to AI-mediated decisions. India may borrow comparative models like the EU's rights-based AI regulatory framework and UNESCO ethical guidelines to ensure AI governance meets constitutional norms, protects human dignity, and promotes social inclusiveness.

## 6. Accountability and Liability in AI Governance

The incorporation of Artificial Intelligence (AI) in governance shifts the old paradigms of accountability, posing tough questions of responsibility, liability, and regulation. In contrast to traditional administrative hierarchies where actors are identifiable, AI-governance obfuscates the different actors between developer, deployer, user, and the state. This diffusion of responsibility requires a careful comprehension of legal frameworks, constitutional obligations, and comparative models so that accountability is not sacrificed in the interests of technological efficiency.

### 6.1 Constitutional and Statutory Legal Accountability

Accountability in governance in India is largely defined by constitutional precepts and doctrines of administrative law. Articles 14 and 21 of the Constitution ensure equality and the right to life and provide a normative standard against which administrative actions based on AI need to be judged. For example, if an AI system misdenies social welfare benefits to marginalized citizens, the state would be liable under the doctrine of constitutional torts, as accepted , which held the state liable for negligence causing harm[19].

Statutory guidelines also guide accountability in AI situations. The Information Technology Act, 2000 places a responsibility on intermediaries (Sections 43A, 66, 69) for maintaining data security and lawful processing. Likewise, the Digital Personal Data Protection Act, 2023 sets fiduciary obligations for entities that process personal data with a focus on consent, purpose limitation, and accountability. Although the statutes themselves do not directly regulate

[19] Nilabati Behera v. State of Orissa (1993)

algorithmic decision-making, they offer a point of departure for laying responsibility when AI systems impact governance decisions.

Judicial oversight has placed in relief the intersection of accountability and legality. The Supreme Court reinforced that any action by the state that affects privacy needs to meet proportionality and necessity, emphasizing that AI surveillance or algorithmic decision-making cannot function in an ethical vacuum[20]. Accordingly, legal responsibility is both a procedural and substantive issue, necessitating compliance with constitutional principles while meeting the specific challenges that AI presents.

### 6.2 Diffusion of Responsibility: Developer, Deployer, User, or State

AI systems are multi-actor collaborative constructs with a diffusion of responsibility. Developers create algorithms, deployers put systems into governance, users interact with interfaces, and the state offers institutional sanction. Liability in the event of harm is ethical and legal entanglement.

In comparison, the EU AI Act of 2024 imposes strict liability on deployers of high-risk AI systems, mandating conformity assessment and risk reduction. The United States, on the other hand, depends on current tort regimes, focusing on negligence and protection of consumers, but not having a coordinated approach to AI responsibility. China's Social Credit System consolidates liability in the state and focuses on control rather than redress at the individual level.

In India, this diffusion makes enforcement more difficult. For instance, if an algorithm incorrectly labels a person as high-risk, is the software developer, police agency, or state to be held liable? Through application of the doctrine, responsibility must ultimately lie with the state as the sovereign body liable for violation of rights, while mechanisms can attribute contributory responsibility to developers or deployers through regulatory mechanisms[21].

### 6.3 Comparative Legal Models: Strict Liability vs. Fault-Based Liability

Two models of liability have emerged in response to AI harms on a global scale. Strict liability assigns responsibility regardless of fault, in order that victims can access redress without

[20] K.S. Puttaswamy v. Union of India (2017)
[21] Nilabati Behera and the E.P. Royappa v. State of Tamil Nadu (1974)

having to establish negligence. The EU's high-risk AI provisions are one such example. Fault-based liability, on the other hand, involves establishing negligence or intent, as in the case of United States sectoral regulation and tort law.

India's existing paradigm is largely fault-based, with principles like administrative negligence and vicarious liability forming the basis of state accountability. However, the opacity of AI makes fault-based systems challenging, as causality is hard to determine. To achieve good governance, India might require a hybrid model: strict liability for high-risk AI systems in policing, welfare distribution, and judiciary assistance, while maintaining fault-based systems for less-risky applications. This would serve the purposes of redress to citizens and proportionate responsibility for implementers.

### 6.4 Suggested Accountability Models for India

There ought to be a strong accountability framework for AI governance in India that incorporates constitutional requirements, statutory obligations, and international standards. Some of the key features could be:

1. Human-in-the-loop requirement: That AI decisions affecting rights or liberty be checked and ratified by human authorities, promoted under the EU AI Act and UNESCO ethical standards.

2. Algorithmic audits: Requiring regular independent reviews to detect biases, mistakes, or disproportionate effects, as suggested.[22]

3. Liability apportionment: Explicitly defining responsibility among deployers, developers, and state agencies, with the state ultimately held responsible for violations of constitutional rights.

4. Transparency and explainability: Requiring public authorities to record algorithmic reasoning and making citizens available explanations for decisions impacting their rights.

5. Redress mechanisms: Creating specific grievance redressal bodies for AI harms, perhaps under a central AI Regulation Authority, as suggested in policy and judicial suggestions.

### 6.5 Ethical and Societal Dimensions of Accountability

Accountability is not only legal; it is also ethical. AI governance is required to guarantee that

[22] Narendra Kumar Goswami v. Union of India (2025)

decisions are in accordance with human dignity, equality, and fairness, in line with constitutional promises. Ethical accountability involves anticipatory identification of potential harms, participatory design of AI systems, and safeguards to ensure that marginalized groups are not excluded. The social dimension emphasizes trust: citizens will be more willing to accept AI governance if the mechanisms are available to correct mistakes, provide explanations of decisions, and assign responsibility openly.

### 6.6 Towards Integrated Governance Accountability

To summarize, AI accountability in governance demands an integrated model integrating legal, ethical, and societal aspects. Indian jurisprudence provides core principles, and comparative experiences present practical approaches. By integrating these principles into statutory amendment, judicial oversight, and policy guidelines, India can make sure that AI-governance promotes efficiency without undermining constitutional accountability. This stance fits into the larger objective of finding a balance between responsibility and innovation so that AI becomes an instrument of empowerment and not one of unbridled destruction.

## 7. Judicial Approaches and Case Studies

The tangible implications of Artificial Intelligence (AI) in government are most clearly understood in the context of specific case studies. Legal, ethical, and social issues take different forms based on jurisdictional settings, technological applications, and governance agendas. Comparing Indian and overseas experiences sheds light on lessons to design resilient AI governance regimes that serve innovation and responsibility in balance. This chapter consolidates judicial orientations, legislative responses, and actual implementation to deduce lessons applicable to India and international governance.

### 7.1 India: AI and Governance in Practice

India's attempt at AI governance has spanned biometric identification, predictive policing, and administrative automation. The Aadhaar initiative, regulated by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, is one of the most ambitious uses of AI and automation in governance. The Supreme Court recognized the efficiency advantage of Aadhaar while underscoring constitutional protections. The Court focused on proportionality, protection of data, and circumscription of state discretion,

inherently placing higher standards of accountability on algorithmic rule-making.[23]

Facial recognition systems used by the Delhi Police provide another meaningful example. Civil society protests and petitions created concerns with privacy, consent, and abuse. Although no final Supreme Court judgment has been delivered, High Court interventions and recommendations from expert committees point to the need for ethical monitoring, human checking, and publicity. The developing jurisprudence demonstrates that Indian courts are slowly acknowledging AI as a governance actor that needs to be conformable to constitutional principles under Articles 14, 19, and 21.

Also, AI-powered welfare distribution platforms have raised serious social issues. For example, Aadhaar-linked ration schemes sometimes led to exclusion of vulnerable groups, setting forth the intersection of legal liability and moral responsibility. Such cases cumulatively illustrate that there is a need to position governance innovations within strong accountability systems to avoid systemic harm.

### 7.2 European Union: Rights-Focused Judicial Oversight

The European Union presents an alternative model, linking statutory precision with judicial enforcement. The General Data Protection Regulation (GDPR, 2016) and the AI Act (2024) represent a rights-based framework governing high-risk AI uses in government. Judicial and administrative rulings under GDPR, including cases on automated credit scoring and algorithmic discrimination, have uniformly applied transparency, human review, and redress rights.

For instance, the Scherms II ruling (Data Protection Commissioner v. Facebook Ireland, 2020) reaffirmed data sovereignty and responsibility in algorithmic regulation, requiring automated processes to abide by privacy and enable effective oversight. These rulings show how codified responsibilities, along with judicial vigilance, avoid algorithmic arbitrariness while ensuring citizens' rights—a lesson that Indian jurisdictions need to learn.

### 7.3 United States: Algorithmic Bias and Judicial Interventions

In the United States, judicial oversight of AI in government has focused mostly on algorithmic

[23] K.S. Puttaswamy (Aadhaar-5J) v. Union of India (2018)

fairness and bias. COMPAS (State v. Loomis, 2016) uncovered racial bias in AI-driven sentencing, which raised due process issues. The courts placed particular importance on transparency and the ability to appeal algorithmic outcomes, even when legislative approaches continued to be sectoral and non-obligatory.

Equally, the Chicago Police Department's pilot predictive policing was criticized publicly for mainly targeting minority groups. Public hearings and policy amendments and limited judicial interference underscored the operation of accountability mechanisms outside the formal legal adjudicative process, demonstrating how law, ethics, and social forces interacted to control AI governance.

### 7.4 China: State-Centric Surveillance and Governance Concerns

The Social Credit System in China is an example of a state-centric AI governance approach. Algorithms combine monitoring data to rank citizens' behaviour, impacting access to public services and social benefits. While the system ensures administrative effectiveness, it triggers serious ethical and legal issues about privacy, autonomy, and basic rights. China's control measures, like the Measures for the Administration of Algorithmic Recommendation (2022), aim at regulating algorithmic providers instead of protecting individual rights, radically different from rights-centred approaches in the EU.

For India, China's case is a lesson in caution: AI could make the government more efficient but needs to be attuned to democratic values and constitutional protections. Complete dependence on state control could erode civil liberties and social trust.

### 7.5 Comparative Insights and Lessons for India

A comparative analysis of these case studies provides several key lessons for India:

1. Constitutional Anchoring: Each AI regulation effort has to be consistent with essential rights. Indian courts have repeatedly enforced proportionality, non-arbitrariness, and reasonableness (Puttaswamy, 2017; Maneka Gandhi v. Union of India, 1978).

2. Transparency and Explainability: EU and U.S. law emphasizes ensuring explainability of algorithms so that citizens may challenge automated decisions.

3. Human-in-the-Loop Mechanisms: Judicial monitoring across jurisdictions puts a premium on having human oversight for decisions with significant impacts, reducing risks of bias and error.

4. Ethical and Social Responsibility: Deployment of technology needs to consider marginalized communities, avoiding exclusion or discriminatory results. Governance frameworks of AI must have integrated ethical audits, participatory design, and grievance redress mechanisms.

5. Regulatory Translucency: Disjoint policies, as in India, raise uncertainty. Organized statutory frameworks, borrowed from the EU AI Act, with flexible soft-law mechanisms are required to provide accountability without over-regulating innovation.

### 7.6 Towards a Holistic AI Governance Model

The confluence of Indian and global experiences proves that sound accountability of AI demands convergence of law, ethics, and public oversight. The judiciary, parliament, and administrative bodies have to work together to ensure that AI systems uphold human rights, are transparent, and offer redressal mechanisms. India can create an inclusive, responsible, and constitutionally aligned model of AI governance by adopting best practices from around the world and striking a balance between innovation and democratic legitimacy.

## 8. Future of AI, Law, and Governance

The path of Artificial Intelligence (AI) in governance promises transformative potential but also highlights the imperative of visionary legal, ethical, and societal frameworks. New technologies hold the promise of efficiency, predictive power, and responsive delivery of public services; but short of total regulation, governance threatens arbitrariness, exclusion, and system bias. This chapter explores future-oriented imperatives for AI law and governance, setting forth holistic strategies for India while learning lessons from international trends.

### 8.1 Requirement for Overall AI Legislation in India

India's existing AI governance structure is dispersed across the IT Act, DPDP Act, sector policies, and proposed national AI strategies. These tools deal with individual elements like data privacy and cybersecurity but fail to deliver a single-statute regime for high-risk AI use in the administration. Upcoming AI interventions like predictive policing, e-justice systems, and

social welfare automation demand legal clarity regarding liability, transparency, human oversight, and accountability.

Comparative lessons from the EU AI Act (2024) demonstrate the merits of a risk-based statutory framework. By categorizing AI systems as unacceptable, high, limited, and minimal risk, the EU guarantees that high-risk governance applications are subject to strict standards of transparency, explainability, human oversight, and compliance auditing. India can follow this framework by incorporating constitutional protections under Articles 14, 19, and 21 to ensure that gains in efficiency do not undermine equality, freedom, or privacy.

### 8.2 The Place of Soft Law, Ethical Guidelines, and Regulatory Sandboxes

Though statutory reform is necessary, working instruments such as soft law and ethical guidelines will continue to be important for India's regulation of AI. Soft law tools—such as OECD AI principles (2019) and UNESCO Recommendation on the Ethics of AI (2021)—offer normative guidance on fairness, accountability, human-centred design, and inclusivity.

Regulatory sandboxes, as encouraged in areas such as fintech, provide India with the chance to test AI governance innovation through contained environments, weighing risk against learning. These sandboxes can promote cooperation among policymakers, technologists, and civil society so that iteratively developed legally compliant, ethically sound AI systems can be created. The test is how to embed these innovations in a wider legal and ethical framework, avoiding ad hoc or concealed deployment.

### 8.3 Balancing Innovation and Accountability

One of the core issues for the future regulation of AI is how to sustain the thin balance between encouraging innovation and guaranteeing accountability. Too much oversight could be stifling to technological testing, but too little creates the danger of constitutional and social damage. The answer is a graduated system in which high-risk applications, like predictive policing, AI adjudication, and biometric welfare systems, are held to rigorous standards of human supervision, independent auditing, and transparency requirements, while low-risk systems have relative leeway.

Judicial precedents, e.g., K.S. Puttaswamy v. Union of India (2017), affirm the precept that efficiency cannot be allowed to supersede basic rights. Legal and moral modalities must thus

be interwoven: accountability is not only punitive but proactive, anticipatory, and participatory.

### 8.4 Human-Centric Governance: Keep Humans in the Loop

One of the most important principles for governing future AI is human-centricity. Human oversight allows automated decisions to be challenged, placed in context, and subject to ethical review. Processes like human-in-the-loop protocols, explainable AI architectures, and open grievance redress mechanisms will be necessary to ensure constitutional values.

Global models, like the EU's mandating human examination of high-risk AI, offer teachable moments. In India, the inclusion of human monitoring is most necessary in light of varied social and economic realities, risks of algorithmic exclusion, and constitutional promises of equality, privacy, and dignity. Human-based governance ensures AI complements human judgment, enhancing legitimacy and trust in the state.

### 8.5 Global Harmonization of AI Governance

AI technologies are by nature transnational, spanning jurisdictional lines and posing questions of regulatory coordination. Governance in the future will need world harmonization of standards, such as common ethical norms, interoperable compliance standards, and collaborative enforcement arrangements. India can use its membership in OECD, UNESCO, and G20 deliberations to reconcile domestic AI regulation with international best practices, providing compatibility, accountability, and global legitimacy.

Additionally, harmonization has to consider cross-border data flows, algorithmic transparency, and ethical compliance, establishing an environment in which innovations created in one jurisdiction do not infringe rights or obligations in another. This cooperation is necessary for India to emerge as a responsible AI innovator in governance.

### 8.6 Policy and Legislative Recommendations

In the future, India must adopt a multi-faceted approach for AI governance:

1. Dedicated AI legislation: An extension of IT Act and DPDP Act, covering liability, risk categorization, transparency, and human review.

2. Ethical framework: Formalizing UNESCO and OECD guidelines into binding policy

directions for state bodies.

3. Regulatory sandboxes: Controlled testing to evaluate effects of AI governance regimes.

4. Algorithmic auditing and impact assessments: Regular reviews for high-risk AI uses to avoid bias, exclusion, or constitutional infringement.

5. Citizen participation and grievance redress: Redress mechanisms for challenging algorithmic decisions and upholding democratic accountability.

6. Global alignment: Collaboration with global authorities to harmonize standards and exchange accountability frameworks.

This holistic approach aims to balance innovation with accountability, ensuring that AI stewardship enhances administrative effectiveness but safeguards constitutional rights and social well-being.

**Conclusion**

Artificial Intelligence (AI) has grown to be a revolutionary driver in government, promising unparalleled levels of administrative effectiveness, predictive policy-making, and citizen-focused service provision, but its implementation raises fundamental socio-legal and ethical issues that require a holistic and people-centred treatment. The study shows that while AI may improve public service delivery via technologies like Aadhaar-based welfare disbursement, e-justice portals, and predictive policing, it also runs the risk of algorithmic bias, discrimination, and exclusion of vulnerable sections, with implications under Articles 14, 19, and 21 of the Indian Constitution. Judicial decisions such as Maneka Gandhi v. Union of India (1978), K.S. Puttaswamy v. Union of India (2017), and Nilabati Behera v. State of Orissa (1993), highlight that equity, proportionality, openness, and accountability should be the foundation of AI-governance, reiterating that effectiveness cannot come at the cost of fundamental rights. Comparative analysis underscores that the European Union, through legislation like the GDPR (2016) and the AI Act (2024), imposes strict transparency, human control, and strict liability on high-risk AI systems, whereas U.S. case law, as represented by State v. Loomis (2016), emphasizes confronting algorithmic bias as well as safeguarding due process even in sectoral regulation scenarios, and China's Social Credit System reflects the risks of monopolizing AI governance without strong protections for individual rights. Holding people accountable in

India is a priority issue with the diffusion of responsibility between developers, deployers, and the state; existing legislation like the IT Act, 2000, and the Digital Personal Data Protection Act, 2023, establishes baseline obligations for data protection and fiduciary duties but fails to hold people accountable for automated decision-making, requiring a hybrid model that compiles strict liability for high-risk AI deployment and fault-based standards for low-risk systems. Ethical leadership, human-in-the-loop processes, algorithmic audits, and participatory design are essential to guarantee that AI supports and supplements human judgment, maintains social trust, and avoids exclusion or injury to at-risk populations. Forward-looking suggestions include passing a specialized AI law that unifies sectoral regulations, putting in place ethical guidelines consistent with UNESCO and OECD standards, making algorithmic explanation and transparency mandatory, creating regulatory sandboxes for controlled testing, applying grievance redressal mechanisms, and achieving global harmony in AI regulation standards to align domestic regulations with global best practices. Through a combination of legal clarity, ethical oversight, societal accountability, and constitutional protection, India is able to develop a governance model that uses AI for administrative efficiency, predictive policymaking, and inclusive citizen participation without compromising on fundamental rights, human dignity, and social equity. Ultimately, the AI of the future in governance depends on finding a judicious balance between innovation and responsibility, inculcating law, ethics, and societal values at all levels of policy formulation and application, thus making India a world leader in responsible, rights-based, human-centred AI governance.