FROM DIGITAL GOVERNANCE TO ALGORITHMIC POWER: ACCOUNTABILITY GAPS IN INDIA AND LESSONS FROM THE EUROPEAN UNION AND THE UNITED STATES

Khushboo Rani, B.A. LL.B. (Hons.); Amity Law School, Amity University Patna

ABSTRACT

The growing use of artificial intelligence (AI) in governance and institutional decision-making raises important questions concerning accountability, constitutional rights and the protection of human dignity. Although AI can improve administrative efficiency and public service delivery, algorithmic systems may also produce discriminatory outcomes, reduce transparency and make it difficult for affected individuals to understand or challenge consequential decisions. The central research problem of this paper is whether existing legal and regulatory frameworks adequately address these accountability gaps while enabling responsible technological innovation.

The paper aims to examine the relationship between algorithmic power, digital governance and human rights, with particular reference to India and comparative developments in the European Union and the United States. It adopts a doctrinal and comparative legal methodology, relying on constitutional provisions, legislation, judicial decisions, international human rights instruments and official policy documents. The analysis considers constitutional protections under Articles 14, 19 and 21 of the Indian Constitution, India's emerging AI governance framework, the European Union's risk-based regulatory approach, and the comparatively sectoral and institutionally fragmented approach of the United States.

The paper argues that responsible AI governance requires more than ethical principles or general commitments to transparency. Effective protection depends on clear allocation of responsibility, proportionate safeguards, meaningful human review, accessible complaint mechanisms and effective remedies for individuals affected by harmful automated decisions. The comparative analysis highlights the importance of distinguishing between formal regulatory commitments and practical mechanisms for enforcing accountability. Accordingly, the paper proposes a rights-based framework for India that integrates constitutional principles with risk assessment, independent scrutiny and procedural fairness.

The paper concludes that technological innovation and human rights protection should not be treated as competing objectives. Rather, accountability, equality, transparency and respect for human dignity should form essential conditions of legitimate and inclusive digital governance.

Keywords: Artificial Intelligence; Digital Governance; Algorithmic Accountability; Human Rights; Constitutional Law; Comparative Regulation; Digital Justice.

1. INTRODUCTION

Artificial intelligence has gradually moved from the field of technical experimentation into the ordinary functioning of society. It is used to recommend content on digital platforms, detect financial fraud, assist medical professionals, evaluate job applications, generate legal documents and support public administration. Governments increasingly rely on digital systems to distribute benefits, manage records, identify suspected irregularities and improve the delivery of public services. These developments have made technology an important part of modern governance.

However, the growing use of AI raises a question that cannot be answered by technological efficiency alone: what happens when a system makes, recommends or substantially influences a decision that affects a person's rights, opportunities or access to essential services? An algorithm may appear neutral because it operates through data and mathematical calculations. Yet its outputs can reflect incomplete information, historical discrimination, poorly designed objectives or assumptions that are difficult for an ordinary person to identify.

Consider a hypothetical situation in which an automated system flags a citizen's application for a public benefit as suspicious. The application is delayed or rejected, but the person receives no meaningful explanation. The official responsible for the decision relies on the system's assessment, while the organization that developed the system treats its technical model as confidential. The affected individual is left uncertain about what went wrong and how to challenge the outcome. The problem in this situation is not simply that the technology may have made a mistake. It is that the decision-making process may lack transparency, responsibility and an effective means of correction.

This example illustrates the relationship between AI and what may be described as *algorithmic power*. Algorithmic power refers here to the capacity of computational systems to influence

decisions, allocate opportunities, classify individuals and shape the exercise of institutional authority. It is not a separate legal power formally recognized by constitutional law. Rather, it is a useful concept for understanding how technological systems can affect the practical exercise of power by governments and private organizations.

The legal significance of this development is particularly clear in India. Articles 14, 19 and 21 of the Constitution protect equality, specified freedoms and life and personal liberty. The Supreme Court's decision in ***Justice K.S. Puttaswamy (Retd.) v. Union of India*** recognised privacy as a fundamental right and connected it with liberty, dignity and autonomy. These constitutional principles provide an important basis for evaluating digital governance, even though they do not automatically resolve every question raised by AI.

India has also adopted the Digital Personal Data Protection Act, 2023, and released the India AI Governance Guidelines in November 2025. The latter promote safe, responsible and inclusive AI adoption while relying substantially on existing legal and regulatory institutions. These developments demonstrate that AI governance is already part of India's policy and legal landscape. The important question is whether the available safeguards adequately address the specific risks arising from algorithmic decisions.

A comparative perspective is necessary because AI systems operate across national borders, and the regulatory choices of one jurisdiction can influence others. The European Union has adopted a comprehensive, risk-based framework through the Artificial Intelligence Act, while the United States has relied on a combination of existing laws, sector-specific regulation and executive policies, with its approach subject to continuing political and administrative change. Neither model can simply be transferred to India without considering constitutional structure, institutional capacity, economic conditions and social diversity.

This paper argues that the legitimacy of digital governance should be assessed not only by the efficiency of the technology employed but also by the fairness of the process, the clarity of responsibility and the availability of effective remedies. Its central concern is the accountability gap that may arise when consequential decisions are shaped by systems that affected individuals cannot adequately understand or challenge.

The paper therefore examines the Indian constitutional and regulatory position, compares selected approaches in the EU and the US, and proposes practical safeguards for rights-

respecting digital governance. Its contribution is normative: it develops a framework for assessing when AI-assisted decision-making requires stronger procedural and institutional protection, rather than assuming that every use of AI is inherently harmful or that all automated decisions should be prohibited.

2. RESEARCH OBJECTIVES AND RESEARCH QUESTIONS

2.1 RESEARCH OBJECTIVES

The principal objective of this study is to examine whether existing legal frameworks provide adequate protection against human rights violations associated with AI-driven digital governance.

The specific objectives are:

1) To analyze the relationship between algorithmic decision-making, public power and fundamental rights.

2) To examine the relevance of Articles 14, 19 and 21 of the Indian Constitution to AI-assisted decision-making.

3) To compare India's approach with selected regulatory developments in the European Union and the United States.

4) To identify gaps relating to transparency, responsibility, procedural fairness and access to remedies.

5) To propose a practical, rights-based framework for accountable AI governance in India.

2.2 RESEARCH QUESTIONS

The study is guided by three principal questions:

- Are existing legal safeguards sufficient when AI systems influence decisions affecting individuals' rights and access to public services?

- What lessons can India draw from the regulatory approaches of the European Union

and the United States?

- Which institutional and procedural safeguards would make AI-assisted governance more transparent, fair and accountable?

3. RESEARCH METHODOLOGY

This paper adopts a doctrinal and comparative legal research methodology. Doctrinal research is used to interpret constitutional provisions, legislation, judicial decisions and relevant international legal instruments. The comparative component examines selected aspects of the Indian, European Union and United States approaches to AI governance, with particular attention to accountability and human rights protection.

The principal primary sources include the Constitution of India, the Digital Personal Data Protection Act, 2023, relevant Supreme Court judgments, the EU Artificial Intelligence Act, the General Data Protection Regulation and international human rights instruments. Official policy documents, including India's AI Governance Guidelines, are also considered to understand the direction of regulatory development.

Secondary materials, including academic scholarship and legal commentary, may be used to explain emerging concepts and evaluate the effectiveness of different regulatory approaches. Particular attention is given to the distinction between binding legal obligations, non-binding policy guidance and recommendations advanced by researchers.

The study is analytical rather than empirical. It does not claim to measure the actual frequency of algorithmic discrimination or establish statistical conclusions about the performance of AI systems. Instead, it evaluates the legal safeguards available to address foreseeable risks. Its comparative scope is necessarily selective: the paper focuses on principles and institutional arrangements relevant to the research questions rather than attempting an exhaustive account of every AI-related law in the three jurisdictions.

The methodology has one important limitation. AI technology and its regulation are developing rapidly. Consequently, legal provisions, implementation dates and policy positions must be verified as of the final date of submission. The conclusions are therefore directed towards a defensible legal framework, while recognizing that further empirical research would be useful in assessing how effectively such safeguards operate in practice.

4. FROM DIGITAL GOVERNANCE TO ALGORITHMIC POWER: CONCEPTUAL AND THEORETICAL FOUNDATIONS

4.1 MEANING AND SCOPE OF DIGITAL GOVERNNCE

Digital governance refers to the use of digital technologies, information systems and online platforms in the administration of public affairs and the delivery of services. It includes online government portals, digital identity systems, electronic records, automated processing and technology-assisted decision-making. Its purpose is often to make public administration more accessible, efficient and responsive.[1]

AI introduces a further dimension. Unlike a conventional database that stores or retrieves information according to predefined instructions, some AI systems can identify patterns, generate predictions or produce recommendations based on data. When such systems are integrated into public administration, they may influence how officials identify risks, prioritize applications or determine which cases require further investigation.

It is important, however, not to treat every digital service as an AI system. A basic online application form may digitize an existing administrative process without using AI. An algorithm that predicts the likelihood of fraud, by contrast, may influence how an application is assessed. The legal questions depend on the system's actual function, the significance of its output and the extent to which people rely on it.

Digital governance can improve access to services, but it can also create new forms of exclusion. A system that assumes access to a smartphone, reliable internet connectivity, digital literacy or standardized language may disadvantage individuals who lack those resources. The quality of governance must therefore be assessed not only by the speed of processing but also by whether people can access services fairly and challenge errors.[2]

4.2 ALGORITHMIC POWER AND THE TRANSFORMATION OF STATE AUTHORITY

Traditional administrative law generally assumes that public decisions are made by identifiable

[1] NITI Aayog, *Responsible AI: Approach Document for India—Part 1: Principles for Responsible AI* (Feb. 2021), https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.
[2] NITI Aayog, *Responsible AI: Approach Document for India—Part 2: Operationalizing Principles for Responsible AI* (Aug. 2021), https://www.niti.gov.in/node/463.

authorities exercising powers conferred by law. The decision-maker must act within legal limits, consider relevant factors and comply with applicable procedural requirements. An affected person may challenge unlawful action before an appropriate administrative body or court.

AI-assisted decision-making complicates this picture. An official may rely heavily on a system whose internal reasoning is difficult to interpret. A private contractor may design the system, a public department may purchase it, and an individual officer may formally approve the final decision. Responsibility is therefore distributed among several actors.

The presence of technology does not eliminate the legal responsibility of a public authority. If a government department uses an automated tool to assist its work, it must still act within the law. It cannot make an unlawful decision lawful merely by explaining that a computer recommended it.[3]

The deeper concern is that algorithmic outputs may acquire an appearance of objectivity. Officials may assume that a numerical score is more reliable than human judgment simply because it is produced by a technical system. Yet a model's output depends on its training data, design choices, assumptions and intended purpose. A numerical result may conceal uncertainty rather than eliminate it.

Algorithmic power is therefore best understood as a challenge to the practical exercise of existing legal authority. It does not require the recognition of a new constitutional power. Instead, it requires legal institutions to examine how established powers are exercised when technical systems influence the process.

4.3 THE ROLE OF PRIVATE TECHNOLOGY COMPANIES

Modern digital governance frequently depends on privately developed software, cloud infrastructure, data analytics and AI services. Governments may not possess the technical expertise required to develop every system internally, making private providers important participants in public administration.

This relationship creates a potential accountability problem. A public authority remains

[3] *Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248 (India).

responsible for the legality of its decisions, but the technical information needed to assess a system may be held by a contractor. Contractual confidentiality, intellectual property claims or restrictions on access to source code may complicate independent scrutiny.[4]

These concerns do not mean that every proprietary system is unlawful or that every source code must be publicly disclosed. Legitimate commercial interests and cybersecurity concerns may justify restrictions on access to some technical information. However, such interests should not automatically prevent a competent authority, court or independent auditor from obtaining the information necessary to examine a serious rights-related complaint.

A sound governance framework must therefore distinguish public disclosure from accountable access. The general public may not need access to an entire model, but an affected individual should receive enough information to understand the essential grounds of a consequential decision. Regulators and courts may require more detailed technical access where necessary.

4.4 THE RULE OF LAW AND HUMAN RIGHTS

The rule of law requires public power to be exercised according to established legal standards rather than arbitrary discretion. In digital governance, this principle requires more than the existence of a software policy or an internal technical manual. The decision must have a lawful basis, pursue a legitimate objective and remain subject to appropriate scrutiny.

Human rights provide the substantive standards against which digital governance should be assessed. Equality requires attention to discriminatory effects. Privacy requires justification for the collection and use of personal data. Freedom of expression may be affected by automated moderation or surveillance. Procedural fairness requires that people have a meaningful opportunity to challenge adverse decisions where the law so demands.

These rights may interact and sometimes create competing considerations. Fraud detection, for example, can protect public resources, while excessive surveillance can intrude upon privacy. The legal question is not whether the government should use technology at all. It is whether the use is lawful, necessary, proportionate and subject to safeguards appropriate to the risks.[5]

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L) 1689.
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

The central principle developed in this paper is therefore straightforward: the use of AI should not reduce the level of legal accountability that would apply if the same decision were made through conventional administrative processes. Where technological complexity makes accountability more difficult, additional safeguards may be needed to preserve effective protection.

5. HUMAN RIGHTS AND CONSTITUTIONAL SAFEGUARDS IN INDIA

5.1 CONSTITUTIONAL FOUNDATIONS: ARTICLES 14, 19, AND 21

The Indian Constitution provides an important foundation for evaluating AI-driven governance. Although it does not contain a provision specifically devoted to artificial intelligence, its existing guarantees are relevant to decisions made or influenced by automated systems.

Article 14 guarantees equality before the law and equal protection of the laws. An algorithm that systematically disadvantages a particular group may raise concerns about arbitrary state action or unequal treatment. The constitutional analysis would depend on the nature of the classification, the purpose of the decision, the evidence of discriminatory effect and the applicable legal standard.[6] Not every difference in algorithmic outcomes automatically amounts to a violation of Article 14, but technical complexity should not prevent judicial examination of potentially arbitrary government action.

Article 19 protects specified freedoms, including freedom of speech and expression under Article 19(1)(a), subject to constitutionally permitted restrictions. Digital systems may affect these freedoms through automated content moderation, online surveillance, account restrictions or systems that influence the visibility of information. Where the state restricts online expression through technology, the restriction must be assessed under the relevant constitutional provisions rather than accepted merely because it is technologically implemented.

Article 21 protects life and personal liberty. The Supreme Court has interpreted this provision broadly, connecting it with dignity, autonomy and fair procedure. In ***Maneka Gandhi v. Union of India***, the Court rejected an isolated understanding of personal liberty and emphasized the

[6] *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 S.C.C. 3 (India).

relationship between Articles 14, 19 and 21. This constitutional approach is significant where AI-assisted decisions affect liberty, access to essential services or other interests protected by law.

These provisions should not be interpreted as establishing a general constitutional prohibition on AI. Rather, they require the use of AI by public authorities to remain consistent with applicable fundamental rights. The constitutional question concerns the nature and consequences of the decision, not merely the technology used to reach it.

5.2 PRIVACY, DIGNITY AND INFORMATION AUTONOMY

In ***Justice K.S. Puttaswamy (Retd.) v. Union of India***, a nine-judge bench of the Supreme Court recognized privacy as a fundamental right protected by the Constitution. The judgment is particularly important for digital governance because personal information can reveal intimate details about individuals, including their activities, associations, preferences and behavior.

AI systems can analyze large quantities of information and draw inferences that were not apparent from the original data. Information collected for one purpose may be combined with other datasets to create profiles used for a different purpose. Even when individual data points appear ordinary, their aggregation may reveal sensitive patterns.

For example, a system might infer a person's financial vulnerability, likely behavior or eligibility for a service by analyzing several sources of information. Such inferences may be inaccurate, but they can still influence how the individual is treated. Privacy protection must therefore consider not only the initial collection of information but also the purposes, inferences and consequences associated with its processing.[7]

The *Puttaswamy* judgment also makes clear that privacy is not absolute. State interference must satisfy constitutional requirements, including legality, a legitimate aim and proportionality. This approach offers a useful framework for evaluating AI systems involving personal information. A government should be able to explain the legal basis for the processing, the public objective being pursued and why the chosen method is appropriate and proportionate.

[7] *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

The Digital Personal Data Protection Act, 2023, establishes a statutory framework for processing digital personal data. Its provisions address matters such as the obligations of data fiduciaries, the rights of data principals and the regulation of personal-data processing. However, data protection and algorithmic accountability are related but distinct questions. Compliance with data protection requirements does not necessarily establish that an automated decision is substantively fair, adequately explained or free from discriminatory effects.

The Act's commencement is also phased, so the applicability of particular provisions must be assessed against the relevant commencement notifications. A paper written in 2026 should not assume that every provision became operational on the date the Act received presidential assent. The official statutory text and subsequent commencement notifications should be consulted when analyzing its present legal effect.

5.3 EQUALITY, NON-DISCRIMINATION AND ALGORITHMIC BIAS

AI systems may reproduce or amplify existing patterns of inequality. This can happen when training data reflects historical discrimination, when certain groups are under-represented, or when a model relies on factors that indirectly correlate with protected or socially disadvantaged characteristics.

Consider a recruitment system trained on historical hiring decisions. If past decisions consistently favored one group, the system may learn patterns that reproduce those preferences. Even if the model does not explicitly use a person's gender or social background, other variables may function as indirect indicators.[8]

This problem is particularly significant in a diverse society such as India. Differences in language, geography, disability, access to technology and quality of available records may affect how accurately individuals are represented in datasets. A system designed around one linguistic or social context may perform less reliably for people outside that context.

The legal response should not assume that all algorithmic differences are discriminatory. A rigorous assessment should examine the purpose of the system, the quality of the data, the effects on affected groups, the availability of less discriminatory alternatives and the

[8] *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1 (India).

justification offered by the decision-maker.

Article 14 provides an important constitutional starting point when state action produces arbitrary or discriminatory outcomes. Where the relevant facts support a claim, other constitutional protections may also be implicated. The challenge is to ensure that a claimant is not denied a meaningful opportunity to establish discrimination simply because the decision was produced through a technical process.

5.4 NATURAL JUSTICE, PROCEDURAL FAIRNESS AND JUDICIAL REVIEW

The principles of natural justice are central to fair administration. Their precise application depends on the statutory context, the nature of the decision and established exceptions. Nevertheless, where a public decision adversely affects a person's interests, questions of notice, an opportunity to respond and an impartial consideration of relevant material may arise.

AI-assisted processes can make these safeguards difficult to exercise. An individual may not know that an automated score influenced the outcome. Even if the individual knows that AI was used, a generic statement that a system detected risk may be insufficient to identify the factual basis for challenging the decision.

Meaningful procedural fairness does not necessarily require disclosure of source code or a complete technical explanation of every model operation. It does, however, require sufficient information for the affected person to understand the essential reasons for the adverse outcome, correct inaccurate information and present relevant objections where the applicable law provides that opportunity.[9]

Human review must also be meaningful rather than ceremonial. If an official merely approves the system's recommendation without considering the individual circumstances, the presence of a human signature may not provide a real safeguard. A reviewer should have the authority, information and competence needed to reconsider the decision.

Judicial review can play an important role where an AI-assisted decision is challenged as unlawful, arbitrary or procedurally unfair. Courts may need to consider expert evidence and

[9] *A.K. Kraipak v. Union of India*, (1969) 2 S.C.R. 457 (India).

technical records, but technical complexity should not make government action immune from legal scrutiny.

The question is how courts can assess the legality of AI-assisted decisions without becoming technical regulators themselves. One answer is to focus on familiar legal questions: whether the authority acted within its powers, relied on relevant information, considered the circumstances, gave adequate reasons where required and provided a fair opportunity to challenge the outcome.

5.5 INDIA'S LEGAL AND REGULATORY FRAMEWORK FOR AI

India's approach to AI governance combines existing legislation, sectoral regulation, institutional initiatives and policy guidance. The India AI Governance Guidelines, released on 5 November 2025, identify principles including trust, people-first governance, fairness, accountability, understandability, safety and sustainability.[10] The guidelines are intended to encourage responsible AI adoption while supporting innovation.

These guidelines are an important development, but their legal character must be described accurately. They should not automatically be treated as equivalent to a comprehensive statute imposing every proposed safeguard as an enforceable legal obligation. Official government explanations indicate that the framework relies substantially on existing laws and sectoral regulators rather than establishing a new horizontal AI law with an entirely new set of statutory mechanisms.

This approach has potential advantages. Existing regulators may already possess expertise in fields such as finance, telecommunications, health and public administration. Building on established institutions can avoid unnecessary duplication and may permit more flexible responses to different uses of AI.

However, a framework based largely on existing laws may leave uncertainty where a particular AI-related harm does not fit comfortably within a specific statutory category. Data protection law may address the processing of personal information, while equality law, administrative law or consumer protection may address other aspects of the same incident. The affected person

[10] Ministry of Electronics & Information Technology, Government of India, *India AI Governance Guidelines* (Nov. 5, 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.

may have to navigate several institutions without a clear understanding of which authority is responsible.

The appropriate conclusion is not necessarily that India must immediately enact a single comprehensive AI statute. The stronger argument is that the effectiveness of the current framework should be assessed against identifiable risks and enforceable remedies. Where existing law provides adequate protection, it should be used effectively. Where important gaps remain, targeted legislation, binding standards or carefully designed regulatory obligations may be justified.

The principal issue is therefore the relationship between innovation and accountability. India's regulatory approach can remain flexible without leaving individuals uncertain about how to challenge serious harm caused by AI-assisted decisions.

6. COMPARATIVE GLOBAL APPROACHES TO AI GOVERNANCE

6.1 THE EUROPEAN UNION: RISK-BASED AI REGULATION AND FUNDAMENTAL RIGHTS

The European Union has developed one of the most comprehensive regulatory frameworks specifically addressing artificial intelligence. Regulation (EU) 2024/1689, commonly known as the AI Act, adopts a risk-based approach under which different obligations apply depending on the type of AI system, its intended purpose and the risks associated with its use.[11]

The basic idea behind this approach is that not every AI application presents the same level of danger. A system used to recommend music does not ordinarily raise the same concerns as one used in recruitment, access to essential services or certain law-enforcement activities. Regulation should therefore be proportionate to the nature and seriousness of the risk.

The AI Act prohibits specified AI practices and establishes requirements for certain high-risk systems. It also addresses general-purpose AI models, transparency and institutional oversight. Its significance lies in its attempt to translate principles of trustworthy AI into a more structured

[11] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L) 1689, https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

set of legal obligations.

The Act's implementation is phased. As of October 2026, the principal prohibitions and AI-literacy provisions have become applicable, and obligations relating to general-purpose AI models have begun to apply. Transparency provisions under Article 50 are scheduled to apply from 2 August 2026. Following the 2026 AI Omnibus changes, certain high-risk obligations have later application dates, including 2 December 2027 for specified high-risk use cases and 2 August 2028 for certain AI systems embedded in regulated products. These dates matter because a regulation's enactment should not be confused with the date on which every substantive obligation becomes enforceable.

The General Data Protection Regulation (GDPR) provides a complementary framework for personal-data processing. Article 22 addresses certain decisions based solely on automated processing that produce legal effects or similarly significant effects for individuals, subject to its conditions and exceptions. The provision includes safeguards in specified circumstances, including opportunities for human intervention and contestation.[12]

The European approach nevertheless has limitations. Risk classification can be difficult where a system has multiple purposes or is used in a changing context. Compliance may also be technically demanding, particularly for smaller organisations. In addition, formal compliance does not automatically ensure that affected individuals can understand a decision or obtain a remedy in practice.

The EU model is valuable for India because it demonstrates how general principles can be translated into differentiated obligations. However, its effectiveness depends on enforcement, institutional capacity and the practical ability of individuals to exercise their rights. India should learn from the model's structure without assuming that the same institutional arrangements would work identically in a different constitutional and administrative context.

6.2 THE UNITED STATES: SECTORAL REGULATION AND INSTITUTIONAL OVERSIGHT

The United States has traditionally approached many AI-related issues through existing legal

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.

regimes, including consumer protection, civil rights, privacy-related rules, employment law and sector-specific regulation. Federal agencies may address harmful practices within their respective statutory powers, while states may adopt additional measures within their constitutional and legislative authority.

This approach can be flexible. Existing institutions may respond to particular harms without waiting for a single comprehensive AI statute. For example, an AI system used in hiring may raise questions under employment discrimination law, while an AI product marketed through deceptive claims may attract consumer-protection scrutiny.

However, a sectoral approach can also produce fragmentation. The applicable rules may depend on the industry, the actor involved, the nature of the harm and the jurisdiction. Individuals and organisations may find it difficult to identify a single, consistent set of obligations applicable across different uses of AI.

The federal policy landscape also changes over time. Executive orders and agency priorities can influence the use and regulation of AI, but they do not all have the same legal status or durability as statutes enacted by Congress. The United States' policy direction as of 2026 reflects continuing efforts to promote AI innovation while addressing security and governance concerns. A careful comparative analysis must therefore distinguish statutory requirements, binding regulations, executive directions and voluntary guidance.[13]

For India, the US experience illustrates both the value and the limits of relying on existing institutions. Sectoral expertise is important, especially where AI applications differ substantially. Yet a purely fragmented framework may leave gaps when a harm crosses institutional boundaries or affects several rights at once.

6.3 INTERNATIONAL HUMAN RIGHTS STANDARDS AND GLOBAL AI GOVERNANCE

AI systems may affect rights recognised under international human rights law, including privacy, freedom of expression, equality and access to an effective remedy. The International Covenant on Civil and Political Rights (ICCPR), for example, protects against arbitrary or unlawful interference with privacy under Article 17 and safeguards freedom of expression

[13] *Ensuring a National Policy Framework for Artificial Intelligence*, Exec. Order No. 14,365 (Dec. 11, 2025), https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

under Article 19. Article 26 addresses equality before the law and equal protection without discrimination.[14]

These provisions were not drafted specifically for AI. Nevertheless, their underlying protections remain relevant when new technologies change the means through which state and private actors exercise influence over individuals. Technological development does not, by itself, remove the need to justify interferences with protected rights.

International standards can also provide a common vocabulary for evaluating governance practices. Principles such as legality, necessity, proportionality, non-discrimination and accountability can guide the assessment of AI systems across jurisdictions, even where domestic regulatory structures differ.

The challenge is that international principles do not always provide a complete operational answer. A general commitment to fairness does not necessarily specify who must audit a system, what information must be disclosed, which authority should hear a complaint or what remedy should follow a violation. Effective governance requires institutions and procedures capable of translating broad standards into practical protection.

International cooperation is therefore important, particularly because AI development and deployment frequently involve multiple countries. Cross-border data flows, cloud services and global platforms can make it difficult to determine which legal system applies and where a complaint should be pursued. Cooperation between regulators, clearer jurisdictional rules and compatible standards can help reduce these difficulties.

At the same time, global harmonisation should not be understood as requiring identical laws everywhere. Countries may reasonably adopt different regulatory methods in response to their constitutional arrangements and social conditions. What matters is that regulatory diversity should not become an excuse for avoiding basic human rights responsibilities.

6.4 COMPARATIVE ASSESSMENT OF INDIA, THE EU AND THE UNITED STATES

The three jurisdictions illustrate different ways of approaching the same central challenge.

[14] International Covenant on Civil and Political Rights arts. 17, 19, 26, Dec. 16, 1966, 999 U.N.T.S. 171.

The EU has adopted a dedicated, risk-based AI regulation alongside its existing data-protection framework. The US approach relies more heavily on sector-specific laws, existing institutions and changing federal policy. India combines constitutional safeguards, general legislation, sectoral regulation and national AI governance guidelines.

These approaches differ in legal form and institutional design, but none eliminates the need to examine the actual operation of AI systems. A detailed statute can be ineffective if enforcement is weak. A flexible framework can leave gaps if responsibility is unclear. Existing laws may provide important remedies, but affected individuals need practical access to them.

For India, the most useful approach may be a combination of these lessons. Risk classification can help prioritise oversight. Existing regulators can contribute sectoral expertise. Constitutional principles can provide a stable foundation, while targeted binding requirements can address gaps that general law does not adequately resolve.[15]

The aim should not be to copy one foreign model. It should be to identify which mechanisms are legally compatible with India's constitutional structure, administratively workable and capable of delivering meaningful protection.

6.5 LESSONS FOR A RIGHTS-BASED GLOBAL FRAMEWORK

Three lessons emerge from the comparison.

First, regulation should be proportionate to risk. AI systems that influence liberty, access to essential public services, employment or other significant interests require closer scrutiny than systems with limited consequences.

Second, legal accountability must remain identifiable. Developers, deployers, public authorities and other participants may have different responsibilities, but the distribution of tasks should not create a situation in which nobody can answer a legitimate complaint.

Third, rights require procedures as well as principles. Individuals need appropriate information, a meaningful opportunity to contest adverse decisions and access to an independent authority

[15] Regulation (EU) 2024/1689, supra note 1; *Ensuring a National Policy Framework for Artificial Intelligence*, Exec. Order No. 14,365 (Dec. 11, 2025); Ministry of Electronics & Information Technology, Government of *India, India AI Governance Guidelines* (Nov. 5, 2025).

where necessary.

A global framework should therefore focus on common minimum safeguards rather than uniform regulation in every detail. This would permit national flexibility while preserving a shared commitment to human dignity, fairness and effective legal protection.

7. ALGORITHMIC POWER, ACCOUNTABILITY GAPS AND DIGITAL INEQUALITY

7.1 THE OPACITY PROBLEM: TRANSPARENCY AND EXPLAINABILITY

One of the most difficult challenges in AI governance is understanding how a system reached a particular result. Some models are technically complex, and their outputs may not be easily translated into a simple explanation. Other systems may be more interpretable but still rely on data or assumptions that are difficult for affected individuals to verify.

Opacity matters because legal accountability depends on the ability to examine a decision. If a person is denied employment, flagged for investigation or refused a public service, a bare statement that an algorithm produced the result may not provide enough information to challenge it.

However, transparency should not be confused with complete public disclosure of every technical detail. Source code may contain commercially sensitive information, security vulnerabilities or details that are not useful to an ordinary person. Publishing it indiscriminately may create new risks without necessarily improving understanding.

A more practical approach is to distinguish several levels of transparency. An affected individual may need a clear statement of the principal reasons for an adverse decision; the important information relied upon and the procedure for challenging it. A regulator may need access to testing records, system documentation and audit results. A court may require more detailed technical evidence when resolving a specific dispute.[16]

This layered approach recognises that different audiences need different information. It also allows legitimate confidentiality interests to be considered without making them an automatic

[16] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), arts. 13–14, 2024 O.J. (L) 1689.

barrier to accountability.

Explainability must be connected to a real legal purpose. A lengthy technical report is of little value if the individual cannot identify an error or obtain reconsideration. Conversely, a concise explanation may be sufficient if it clearly identifies the decisive factors and provides a meaningful route to challenge the outcome.

7.2 AUTOMATED DECISIONS AND THE EROSION OF PROCEDURAL FAIRNESS

The use of AI can change the practical experience of administrative decision-making. Traditional procedures often allow an individual to present documents, explain unusual circumstances or correct inaccurate information. Automated systems may process large numbers of cases efficiently, but they can also treat unusual situations as exceptions that do not fit the model's assumptions.

The problem becomes serious when the system's recommendation is treated as conclusive. If an official assumes that the model is necessarily objective, the person affected may have little opportunity to correct a mistake. Human involvement then exists only in form, not in substance.

A rights-respecting system should distinguish between assistance and delegation. AI may help identify relevant information or highlight possible inconsistencies. But where a decision has serious consequences, the responsible authority should retain the ability and duty to consider individual circumstances and correct the system's output.

This does not mean that every administrative task must be decided manually. Fully automated processes may be appropriate for routine and low-risk functions where the applicable law permits them and adequate safeguards exist. The need for human review should be proportionate to the significance of the decision and the likelihood of harm.

The key principle is that efficiency should not eliminate a fair opportunity to be heard where such an opportunity is legally required or necessary to prevent serious injustice.[17]

[17] *A.K. Kraipak v. Union of India*, (1969) 2 S.C.R. 457 (India).

7.3 SURVEILLANCE, PRIVACY AND THE CONCENTRATION OF DIGITAL POWER

AI can increase the scale and sophistication of surveillance by enabling the analysis of images, movements, communications and behavioural patterns. Some surveillance tools may serve legitimate purposes, including identifying security threats or locating missing persons. Yet their use can also interfere with privacy and chill lawful activities if individuals believe that their behaviour is constantly monitored.

Facial recognition illustrates this tension. Its accuracy may vary across systems and circumstances, and its use may raise concerns about misidentification, disproportionate monitoring and the absence of meaningful safeguards. The legal assessment must consider the specific purpose, the legal authority for deployment, the population affected, the reliability of the system and the availability of less intrusive alternatives.

The concentration of digital infrastructure also deserves attention. When governments depend on a small number of technology providers, public institutions may become reliant on systems they cannot independently assess or easily replace. This dependence can affect procurement decisions, data governance and the practical ability to enforce contractual or regulatory standards.[18]

A proportionate response should combine legal controls with institutional capacity. Authorities need clear rules on permissible uses, retention of data, access restrictions and independent review. Procurement contracts should also preserve the government's ability to audit systems and investigate serious complaints.

Surveillance should not be justified merely by asserting that technology makes monitoring easier. The state must still establish the lawful purpose and justification for intrusive measures under the applicable constitutional and statutory standards.

7.4 ALGORITHMIC DISCRIMINATION AND THE DIGITAL DIVIDE

Algorithmic inequality is not limited to biased datasets. It can also arise from unequal access to technology, language barriers, disability, poor-quality records and differences in the ability

[18] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

to challenge a decision.

In India, a digital service may be formally available to everyone but remain practically inaccessible to individuals who lack reliable connectivity, digital literacy or access to assistance. An automated system may also perform less accurately when processing names, documents or language variations that are poorly represented in its training data.

These problems show why fairness must be evaluated in context. A system that performs well on average may still produce serious errors for a particular group. General accuracy figures may conceal the distribution of mistakes and the consequences they have for different individuals.[19]

Institutions using AI should therefore examine performance across relevant groups, where lawful and appropriate, and investigate significant disparities. Assessments should consider both the quality of the system and the broader process in which it operates. A technically accurate model can still produce an unfair result if the underlying policy is unjust or the decision-making procedure offers no opportunity to correct mistakes.

Accessibility must also be treated as part of effective governance. Alternative methods of applying for a service, human assistance and accessible complaint procedures can prevent digital systems from becoming barriers to rights that individuals are otherwise entitled to exercise.

7.5 FRAGMENTED LIABILITY AND THE ACCOUNTABILITY GAP

AI-related harm can involve several actors. A developer designs a model, a vendor integrates it into a product, a public authority deploys it and an individual official relies on its output. The harm may result from a combination of defective design, unsuitable data, improper deployment and inadequate human oversight.

Traditional legal principles remain relevant, but their application may be complicated by this distribution of responsibility. Negligence, statutory duties, contractual obligations and public-

[19] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019, amended May 3, 2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

law remedies may each address different aspects of a dispute. The relevant route will depend on the facts, the applicable law and the relationship between the parties.

The first mistake would be to assume that the AI system itself automatically becomes the legally responsible person. Current liability analysis generally requires attention to the human or legal entities involved, their duties, their conduct and the causal relationship between that conduct and the harm. Whether a particular entity is liable must be established under the applicable legal regime.

The second mistake would be to place all responsibility on the final human user. An official may reasonably lack the technical capacity to identify a hidden design defect. A developer, in turn, may not control the context in which a system is ultimately used. Responsibility should therefore be allocated according to the actor's role, control, knowledge, legal duties and contribution to the risk.

For public authorities, outsourcing does not remove the duty to act lawfully. A department should not be able to avoid scrutiny by arguing that a private company developed the system. At the same time, developers and vendors should not automatically be held responsible for every unexpected outcome irrespective of their conduct or applicable legal duties.

The practical objective is to prevent accountability from disappearing between institutions. Clear documentation, contractual audit rights, incident reporting, record-keeping and accessible complaint mechanisms can help establish what happened and who had responsibility for preventing it.[20]

7.6 ACCESS TO JUSTICE AND EFFECTIVE REMEDIES IN THE DIGITAL AGE

Legal rights have limited practical value if a person cannot enforce them. AI-related disputes may require technical expertise, access to records and the ability to challenge evidence held by a powerful institution. These demands can be especially burdensome for individuals with limited financial or digital resources.

[20] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019, amended May 3, 2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

An effective framework should provide a clear route for complaints. Depending on the context, this may involve the relevant administrative authority, sectoral regulator, data-protection mechanism, consumer forum or court. The individual should not be expected to understand the entire regulatory structure before discovering where to seek assistance.

Procedures should also account for unequal access to evidence. A person challenging an algorithmic decision may not possess the records needed to demonstrate how the system operated. Appropriate disclosure and independent examination mechanisms can help address this imbalance while protecting legitimate confidentiality and security interests.

Remedies should reflect the nature of the harm. They may include correction of inaccurate data, reconsideration of a decision, restoration of a wrongly denied benefit, compensation where legally available, or an order requiring unlawful practices to cease. Not every dispute will justify every remedy, and the competent institution must apply the relevant legal standards.

The broader point is that accountability must be practical. A right to complain is not meaningful if the complaint process is inaccessible, the relevant evidence cannot be examined or no authority has the power to provide relief.

8. TOWARDS A RIGHTS-BASED MODEL OF DIGITAL GOVERNANCE: FINDINGS AND RECOMMENDATIONS

8.1 A HUMAN RIGHTS-BASED APPROACH TO AI GOVERNANCE

The preceding analysis suggests that the central challenge is not the existence of AI itself, but the conditions under which it is designed, deployed and relied upon. A legal framework should neither prohibit beneficial innovation without sufficient justification nor assume that technological progress automatically produces fair outcomes.

A rights-based approach would begin by identifying the interests affected by a proposed AI system. These may include privacy, equality, freedom of expression, access to public services and procedural fairness. The degree of scrutiny should reflect the seriousness of the possible harm, the vulnerability of affected individuals and the extent to which the system influences the final decision.

For India, this approach should build on constitutional guarantees and existing legislation. The

India AI Governance Guidelines provide an important policy foundation, but the practical question is how their principles can be translated into enforceable obligations where existing law does not provide sufficient protection. Any new requirements should be carefully designed to complement, rather than unnecessarily duplicate, existing regulatory mechanisms.[21]

The first recommendation is therefore to establish a clear legal framework for identifying consequential AI uses and determining which safeguards apply to them. The objective should be proportionate protection, not regulation for its own sake.

8.2 MANDATORY IMPACT ASSESSMENTS AND INDEPENDENT ALGORITHMIC AUDITS

AI systems used in consequential settings should undergo an assessment proportionate to their potential impact. Such an assessment should consider the purpose of the system, the data used, foreseeable errors, possible discriminatory effects, privacy implications and the availability of alternative methods.

For public authorities, an assessment should also address whether the system is necessary for the stated objective and whether the same objective could be achieved through a less intrusive or less risky method. This would connect technological evaluation with the constitutional principles of legality, necessity and proportionality.

Independent audits can complement impact assessments. An audit may examine system performance, data quality, security, compliance with stated requirements and disparities in outcomes. The auditor should possess appropriate expertise and sufficient independence from the organisation being assessed.[22]

Not every low-risk application requires the same level of scrutiny. A proportionate framework could reserve mandatory independent audits for specified high-impact uses or where credible evidence of serious harm exists. Smaller organisations should not face unnecessary procedural burdens when deploying systems with limited consequences.

[21] Ministry of Electronics and Information Technology, Government of India, *India AI Governance Guidelines* (Nov. 5, 2025), https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2186639&lang=2&reg=3.
[22] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) arts. 9, 27, 2024 O.J. (L 1689) 1.

The crucial point is that assessments and audits should not become paperwork exercises. Their findings should lead to corrective action, restricted deployment or withdrawal where serious risks cannot be adequately controlled.

8.3 MEANINGFUL HUMAN OVERSIGHT AND THE RIGHT TO CHALLENGE DECISIONS

Where an AI system substantially influences a consequential decision, affected individuals should have access to an appropriate explanation and a meaningful opportunity to challenge the result, subject to the governing law.

This recommendation does not assume that a universal, unlimited legal right to human review already exists in India. Rather, it proposes that such safeguards should be expressly required in appropriate contexts, particularly where a decision significantly affects legal rights, access to essential services or other important interests.

Meaningful human oversight requires more than placing an official at the end of an automated process. The reviewer must be able to examine the relevant information, understand the limitations of the system, consider individual circumstances and change the outcome where justified.[23]

An effective challenge mechanism should allow a person to identify incorrect data, present relevant evidence and request reconsideration. The explanation provided should be sufficient to make the challenge practical. Where technical complexity prevents a complete explanation, the institution should still disclose the principal reasons and relevant factors to the extent compatible with law and legitimate security interests.

Such safeguards would help ensure that automation supports public administration without eliminating individual agency or procedural fairness.

8.4 TRANSPARENT PUBLIC PROCUREMENT AND INSTITUTIONAL ACCOUNTABILITY

Public procurement is an important point at which accountability requirements can be

[23] Regulation (EU) 2024/1689, supra note 2, art. 14.

established. When a government department acquires an AI system, its contract should address documentation, security, performance testing, data handling, incident reporting and access to information necessary for oversight.

Contracts should also clarify the respective responsibilities of the public authority and the technology provider. Where the system is intended to influence decisions affecting individuals, the authority should retain sufficient access and control to investigate errors and comply with its legal obligations.[24]

Commercial confidentiality should be respected where justified, but it should not prevent lawful regulatory examination or judicial scrutiny. Confidential technical material can be disclosed to authorised reviewers under appropriate safeguards where necessary.

Institutional responsibility must remain clear. Each public body deploying AI should identify the official or unit responsible for monitoring the system, receiving complaints and ensuring compliance with applicable law. Regulators should also have sufficient expertise and resources to evaluate AI-related risks within their respective mandates.

These measures would make accountability part of the system's design and procurement, rather than an issue considered only after harm occurs.

8.5 INTERNATIONAL COOPERATION AND REGULATORY HARMONISATION

Because AI systems and digital services operate across borders, national regulation alone may not resolve every problem. A system may be developed in one country, hosted in another, deployed by an organisation in a third and used by individuals worldwide. Investigations and remedies can become difficult when evidence and responsible actors are located in different jurisdictions.

India should therefore support international cooperation on common technical standards, information-sharing arrangements, cross-border investigations and effective remedies.

[24] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019, amended May 3, 2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

Cooperation could also improve the exchange of expertise among regulators, courts, academic institutions and civil society.[25]

However, harmonisation should not mean that India must reproduce the EU model or follow every change in US policy. Different jurisdictions have different constitutional traditions, institutional capacities and public priorities. International standards should establish useful common protections while allowing legitimate domestic variation.

A balanced model would combine risk-sensitive regulation, effective national enforcement and cooperation on cross-border matters. Such an approach would protect rights without treating technological development as inherently incompatible with public welfare.

8.6 SUMMARY OF THE PROPOSED FRAMEWORK

The recommendations can be organised around six connected safeguards:

Safeguard & Purpose

Risk classification - Direct scrutiny towards AI systems capable of causing serious harm

Impact assessments - Identify risks before deployment

Independent audits - Test reliability, fairness and compliance

Meaningful human review - Preserve procedural fairness in consequential decisions

Clear responsibility and remedies - Prevent accountability gaps and make complaints effective

International cooperation - Address cross-border risks and improve consistency

These safeguards should be understood as a proposed framework, not as a claim that every measure is already mandated by current Indian law. Their precise legal form should be determined through legislative review, consultation and assessment of existing institutional powers.

[25] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019, amended May 3, 2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

The most important finding is that accountability should operate throughout the life of an AI system: before deployment, during use and after a complaint or harmful incident. This would connect preventive regulation with individual remedies and public oversight.

9. CONCLUSION

Artificial intelligence is becoming an important part of digital governance, influencing how information is processed, services are delivered and decisions are made. These developments offer genuine benefits, including greater efficiency, improved access to information and the possibility of more responsive public administration. Yet they also raise difficult legal questions when algorithmic systems influence decisions affecting human rights.

This paper has argued that the central issue is accountability. A person affected by an AI-assisted decision should not be placed in a weaker legal position merely because the decision was influenced by technology. Public authorities must continue to act within constitutional and statutory limits, while private organisations must comply with the duties applicable to their conduct. Technical complexity should not become a reason to deny meaningful scrutiny.

India's constitutional framework, particularly Articles 14, 19 and 21, provides important principles for assessing digital governance. The *Puttaswamy* judgment offers a significant foundation for privacy and autonomy, while data-protection legislation and the India AI Governance Guidelines form part of the evolving regulatory landscape. The comparison with the European Union and the United States shows that different regulatory methods can address AI-related risks, but each depends on effective implementation, clear responsibility and accessible remedies.

The paper's principal recommendation is a proportionate, rights-based framework combining risk assessment, independent scrutiny, meaningful human oversight, transparent public procurement and effective complaint mechanisms. Such a framework should strengthen existing institutions and introduce additional legal obligations where genuine gaps are identified.

Ultimately, responsible digital governance requires more than systems that operate quickly or produce technically sophisticated results. It requires institutions capable of explaining decisions, correcting errors and protecting individuals from arbitrary or discriminatory

treatment. The success of AI governance should therefore be measured not only by technological advancement, but also by whether innovation remains consistent with human dignity, equality and the rule of law.

The challenge for India and the international community is not to choose between AI innovation and human rights. It is to build governance arrangements in which innovation can develop without making accountability an afterthought.