
**ALGORITHMIC GOVERNANCE AND DUE PROCESS:
COMPARATIVE ADMINISTRATIVE LAW RESPONSES IN INDIA,
THE EU, AND THE UNITED STATES**

***Raj Aryan**

Student LL.M. (Master of Laws), Amity Institute of Advance Legal Studies, Amity
University, Noida, Uttar Pradesh, India.

Article Received: 13 August 2026

*Corresponding Author: Raj Aryan

Article Revised: 03 September 2026

India.

Published on: 23 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.8014>

ABSTRACT

Algorithmic government changes the contexts in which administrative law can make public power accountable. This Article examines the challenge that traditional guarantees of notice, reasons, hearing, non-arbitrariness and judicial review may become unavailable, formal or substantive in their absence, when a public decision is made with the aid of hidden data, models or systems under control of vendors. A comparative doctrinal methodology is used to study Indian constitutional and administrative law, along with the EU's data protection and Artificial Intelligence Act and the procedural due process and federalism of the United States. The study shows convergence around five requirements, namely lawfulness, intelligibility, meaningful human review, auditable decision-making records and extensive safeguards to protect against potentially high-impact deployments. While these requirements are dealt with differently by each jurisdiction, there is a strong emphasis on legislation and regulatory requirements in the EU, a strong emphasis on constitutional balance, on court review and on the administrative and executive branches in the United States, and a strong emphasis on Articles 14 and 21, privacy and proportionality and data protection along with an emerging polity in India. While the emphasis is on the Constitution, this Article argues for against transplanting either of the EU or the United States models. Rather, it should be treated as an example of an application of existing public law obligations in the context of algorithms. This approach preserves technological flexibility and improves accountability and judicial review.

KEYWORDS: Algorithmic Governance; Due Process; Administrative Law; Artificial Intelligence; Judicial Review.

1.1 INTRODUCTION

Public administration uses systems that rely on data for almost all decisions about administrative applicant classification, risk detection, resource allocation, identity checks and enforcement. While these systems increase consistency and capacity within public administration, they centralize decision-making power into systems and infrastructure that may leave the persons involved out of the decision context altogether. This can create opacity and determine whether a challenged individual can even recognize an error, understand the decision against them, or remedy the situation. Frank Pasquale's account of opacity within institutions can explain the administrative law problem in these systems. Therefore, administrative law must interrogate the practical consequences of computational reasoning for the preservation of the traditional procedural protections.¹

This is a problem of legal transformation. The old systems of constitutional law and of administration describe identifiable persons, records and reasons. However, the systems we use today may rely on inference, on continuous data processing and models provided by private parties. Mireille Hildebrandt demonstrates that, in systems of administrative agency, data-centered operations can shift the conditions of legal operations in which certainty and redress of the law are guaranteed.² This problem cannot be addressed by requiring a rational human official to affirm a decision by signing a formal order. Similar studies of technocratic governance also indicate that the quality of data and the design of institutions can define limits on what is possible within the system.³

This Article studies India, the European Union and the United States by focusing on India as the main region for doctrinal development. Subjects covered include constitutional fairness, privacy, data protection, automated decision rights, Artificial Intelligence and judicial review focusing on the public interest, biometrics and major uses of government. The main idea is that algorithmic due process should not be considered a right that is unique to technology. Rather, it should consist of legality, non-arbitrariness, rules and the right to be heard, and the right to scrutinize decisions. India possesses the tools for that construction of due process

¹ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3 (Harvard University Press, Cambridge, MA, 1st edn., 2015).

² Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* 133 (Edward Elgar Publishing, Cheltenham, 1st edn., 2015).

³ Marijn Janssen and George Kuk, "The Challenges and Limits of Big Data Algorithms in Technocratic Governance", 33 *Government Information Quarterly* 371 (2016).

automated and integrated in its Constitution, but these need to be safeguarded before, during and after automated decision making.⁴

1.2 CONSTITUTIONAL FOUNDATIONS AND ALGORITHMIC ADMINISTRATION IN INDIA

In the context of India, dispersed answers to algorithmic administration are found in the Constitution, data protection laws and policy directives, as opposed to a single law on Artificial Intelligence. That dispersed approach does not represent a doctrinal gap. Standards that Articles 14 and 21 provide can be used to review computational public power and system design and/or individual case outcomes.⁵

1.2.1 Constitutional Fairness, Non-Arbitrariness and Proportionality

The first doctrinal point is the principle of procedural fairness provided in Article 21 and read with Article 14. In *Maneka Gandhi v. Union of India*⁶, the Court held State action impacting liberty must be fair, just and reasonable. In algorithmic administration, this principle must extend beyond the final communicate of the order. A decision may be legally unsound when the decisive model employs legally irrelevant proxies or hidden criteria or inputs which are wrong or unreliable, even if a decision maker endorses the output of the model. Constitutional review should thus examine the decision process and the structure of official discretion, as well as the challengeable information.

Legal principles for privacy as articulated in *Justice K. S. Puttaswamy (Retired) v. Union of India*⁷, provide the further elements of legality, legitimate purpose, proportionality and informational autonomy. Many Governmental algorithms use massive collection and/or linkage and/or inference of personal data. A system can be accurate from a statistical standpoint, but may still be constitutionally excessive if it collects more personal data than the public purpose justifies or if it collects data for additional, unprotected, or unregulated purposes. Additionally, proportionality mandates consideration of less restrictive alternative means. Courts should evaluate whether the administration's aim justifies the use of a particular technology of invasive personal data collection and whether similar aims might be accomplished with less invasive personal data techniques.

The case around Aadhaar provides useful insights into the potential and constraints of this model of litigating technology. In *Justice K. S. Puttaswamy (Retired) v. Union of India*

⁴ Cary Coglianese and David Lehr, "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era", 105 *Georgetown Law Journal* 1147 (2017).

⁵ The Constitution of India, arts. 14, 21.

⁶ (1978) 1 SCC 248.

⁷ (2017) 10 SCC 1.

(*Aadhaar*)⁸, the Supreme Court assessed the statutory framework on a range of issues related to authentication, exclusion, data retention and proportionality. One of the most important lessons of algorithmic governance is that the rule of law cannot be replaced by the reliability of algorithms. using the example of how automated systems of social control shape the contemporary welfare state, Virginia Eubanks demonstrates how, in the digital age, administrative errors transform from easy to challenge procedural errors to absolute refusals of services. This demonstrates that the Indian legal system requires safety nets to offset the negative consequences of verification processes.⁹

1.2.2 Data Protection and Responsible Artificial Intelligence Governance

The Digital Personal Data Protection Act, 2023, contains rules for lawful processing, notice, data accuracy, security safeguards and the right to correction and erasure. Whilst important, these rights do not build a comprehensive automated administrative law.¹⁰ Data protection rights and administrative reasons are distinct. A person may understand what personal data are processed, but may still have no idea why a model determined that an application posed a risk and was therefore ineligible. Hence, legal certainty should introduce a right to automatic processing, to understand why a model raised a substantial obstacle to the right and to have the decision reviewed.

The principles of safety, equality, inclusivity, privacy, transparency and accountability are recognized in earlier versions of India's Responsible AI. These principles differentiate AI and allow for design of operational mechanisms for responsible deployment prior to deployment.¹¹ Due process provides one means of addressing AI bias, but it is best to address these issues before deployment through model validation, bias testing, data quality assurance, and document design along with the creation of an effective grievance redress mechanical. Principles that inform policies only take legal significance in relation to definable public law obligations. Therefore, for high impact government deployments, an Impact Assessment should identify the legislation and describe the population impacted, the source of the data and the anticipated errors, discrimination, oversight, and the ability to handle individual cases.

The India Artificial Intelligence Governance Guidelines released in November 2025, adopt a principle-based and risk-proportionate approach of trust, design, fairness, accountability,

⁸ (2019) 1 SCC 1.

⁹ Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 12 (St. Martin's Press, New York, 1st edn., 2018).

¹⁰ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 4, 5, 8, 12.

¹¹ NITI Aayog, *"Responsible AI #AIForAll: Approach Document for India, Part 2: Operationalizing Principles for Responsible AI"* (August, 2021).

transparency and safety. Their preference for existing laws and sector mechanisms rather than an immediate horizontal statute keeps the options and procedures for deployment from being too rigid, but this approach may result in different levels of protection being afforded.¹² The preferred approach is to consider these Guidelines as institutional guidance to inform the manner in which public duties are to be fulfilled. For public bodies, the Guidelines should be an express condition of procurement, access, and record keeping and should be covered by audit and assurance that can be challenged under ordinary public law.

1.2.3 Judicial Review of Biometric and Automated Administration

Recent Indian court cases show how legal principles may be applied. In *ONGC Officers Association v. Oil and Natural Gas Corporation Limited and Others*¹³, the Delhi High Court examined a (a) facial recognition technology-based (b) geo-fenced (c) attendance system. The Court declined to strike down the system, yet, recognised the (d) privacy, (e) proportionality, (f) purpose limitation, and (g) excessive tracking issues. The Court's opinion has value because it provides a standard that makes the (d) privacy and (e) proportionality assessment at implementation the determinant of legality. An attendance-related system can become unconstitutional if data collection is extended, tracking is continuous, or the purpose for which the data was collected is broadly interpreted to include administrative purposes that are disconnected from the attendance system.

The size of these systems requires safety measures be implemented without delay. A government report from July 2026 stated that there were 762 government Artificial Intelligence problem statements, 62 ministries, and 62 government departments, in tandem with an emerging training and assurance system. In comparison to responsible Artificial Intelligence, Figure 1 depicts the significant deployment initiatives.¹⁴ The focus should not be on deployment, but rather, assurance should follow the same pace, as the system's purpose is to affect benefits, employment, taxes, licensing, health, policing, or education. Challenges should be integrated into the system itself, rather than implemented after systemic errors occur.

¹² Government of India, Ministry of Electronics and Information Technology, "*India AI Governance Guidelines*" (November, 2025).

¹³ W.P.(C) 5074/2026.

¹⁴ "IndiaAI Mission Advances AI-Driven Governance and Public Service Delivery through Collaborative Roadmaps, Innovation Challenges and Capacity Building", available at: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2291062&lang=1®=3> (last visited on August 24, 2026).

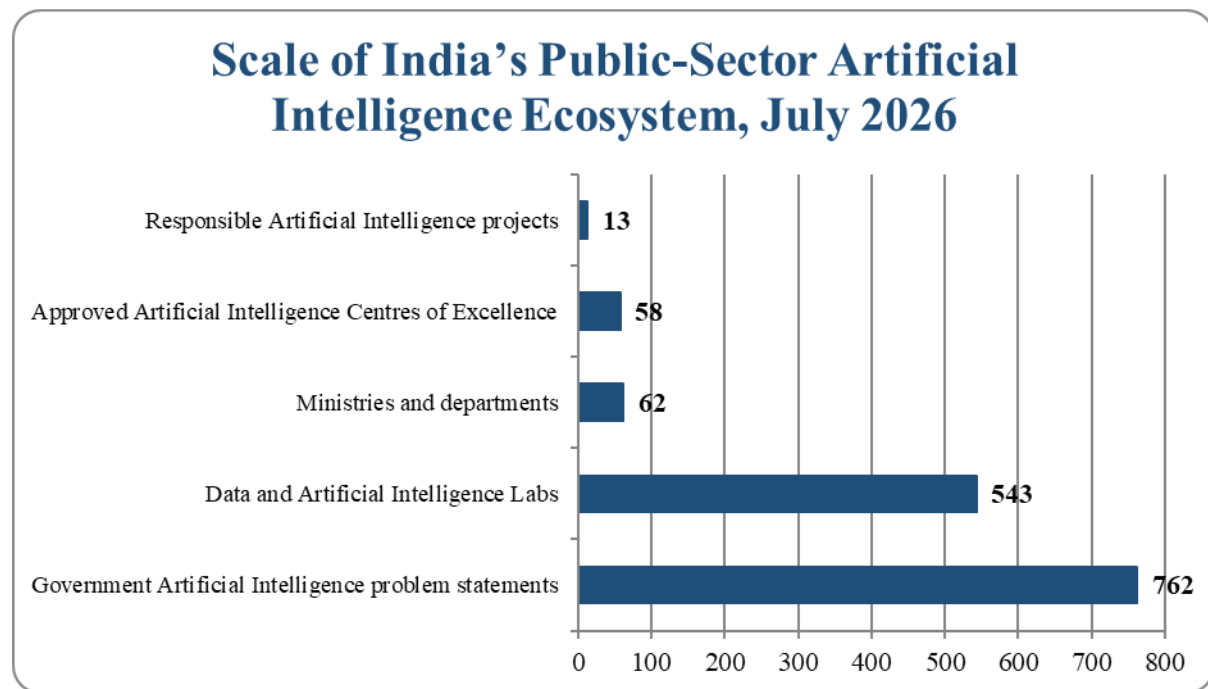


Figure 1. Scale of India's public-sector Artificial Intelligence ecosystem, July 2026.

Source: Press Information Bureau.

1.3 RIGHTS-BASED REGULATION OF AUTOMATED ADMINISTRATION IN THE EUROPEAN UNION

As compared to the other two jurisdictions, the European Union has the most thorough statutory design. Regulations for fundamental rights, data protection and AI legislation interrelate. While this structure still requires some degree of administrative-law reasoning, it moves a number of requirements of fair automated administration from the fairness in administration to requirements that must be satisfied prior to, and after the taking of, an affected administrative decision.¹⁵

1.3.1 Data Protection, Explanation and Contestability

The General Data Protection Regulation (GDPR) offers a procedural layer through the right to information, access, and Article 22 safeguards for automated decisions that have legal or significant effects. The occupational value of the GDPR is in the relationship of information with challenge.¹⁶ The right to object or to appeal is largely meaningless if the person cannot identify the deciding data or logic. The GDPR, however, is not a full code of public-sector due process. The principle of legality requires consideration of the purpose of the statute, the

¹⁵ Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, arts. 8, 41, 47.

¹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) [2016] OJ L 119/1, arts. 13-15, 22.

relevance of the evidence, the reasons and justification for the decision, and the authority of the decision-maker.

Studies on automated administrative decision-making under the General Data Protection Regulation demonstrate the relationship between technological complexity and legally meaningful information. The optimal standard is not complete technological transparency.¹⁷ Source code may be totally incomprehensible to the majority of individuals affected. In such instances, the affected individuals have a right to the decision-relevant information. This would include the key factors, data and rules that substantively influenced the outcome, and would also include enough information to help the affected individuals to identify whether the decision contained a factual error or was weighted unlawfully. This option would not be a false choice between complete disclosure and total secrecy. It would strike a balance between the explanation offered and the administrative reasons for the decision.

1.3.2 The Artificial Intelligence Act as Procedural Infrastructure

Regulation (EU) 2024/1689, the Artificial Intelligence Act, introduces a layer that is risk-based and addresses the prohibition of certain practices, systems of high risk, transparency, documentation, human oversight and monitoring as well as governance after market introduction. Its effects are more significant and substantive than merely classification.¹⁸ Karen Yeung and Martin Lodge define algorithmic regulation as a type of governance that is able to regulate practices while also being subject to regulation. The Act seeks to address this duality by imposing obligations on various stages of the system rather than waiting for a problematic decision to be made. For administrative law, the requirements of data quality, logging, technical documentation and human oversight collectively can provide the evidence to help make reasons for decisions and judicial review more effective.

There is a need for exact timing in the performance of duties. The relevant provisions of the Artificial Intelligence Act commence on 2 August 2026. Rules for Annex III high-risk systems have been simplified for 2026, and provisions will apply until 2 December 2027 for high-risk systems; and until 2 August 2028 for high-risk systems embedded in regulated products.¹⁹ Hence, the model continues to be transitional. India must examine the architecture of IIoT without identifying each high risk obligation as currently applicable. The main structural element is that risk identification, documentation and monitoring, and oversight

¹⁷ Filip Geburczyk, "Automated Administrative Decision-Making under the Influence of the GDPR: Early Reflections and Upcoming Challenges", 41 *Computer Law & Security Review* 105538 (2021).

¹⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act) [2024] OJ L 2024/1689, arts. 5, 9-15, 26, 72.

¹⁹ "The Enforcement Framework of the AI Act", available at: <https://digital-strategy.ec.europa.eu/en/policies/enforcement-ai-act> (last visited on August 24, 2026).

should be conducted prior to a decision that is likely to be adverse, rather than after the decision has been made, and an individual is expected to litigate and reconstruct an opaque system.

1.3.3 Judicial Development of Meaningful Explanation

The Court of Justice has provided some useful clarifications on the boundaries of safeguards for automated decision making. In the case of *OQ v. Land Hessen*²⁰, SCHUFA Holding AG produced a probability score. The Court decided that in such cases automated scoring plays a role in the decision-making process, and therefore is considered an automated individual decision-making process. This is an important consideration for public administration. A body should not avoid its obligations by placing a human official between the algorithm and the command. Rather, the substantive impact of the order should be the primary concern of the review.

The principle began to take shape in the case *CK v. Magistrat der Stadt Wien*²¹, in which a Court decision was given on the right to information to understand and challenge automated credit assessments. The decision of the Court requires that information be made available in order to challenge the decision, with trade secrets and the rights of third parties to be balanced. There is also research on explainable Artificial Intelligence in government, in which the design of explanations influences the perception of fairness and trust of the system. The legal precedent is more restrictive: for a system to be explained, it must allow for the outcome to be challenged, as well as for the legal justification behind the outcome to be explained.²²

The importance of this framework will be more visible when the technology is implemented. The European Commission's mapping showed that in 2025 there were 245 cases of emerging technologies in the public sector across 21 countries, with the vast majority being Artificial Intelligence. Figure 2 provides the breakdown of the technologies.²³ It can be seen that automated systems are becoming a normal part of modernizing the public sector, as opposed to being a temporary measure in public sector regulation. As automated systems penetrate ordinary administrative sectors, the line between technology regulation and administrative

²⁰ Case C-634/21, ECLI:EU:C:2023:957.

²¹ Case C-203/22, ECLI:EU:C:2025:117.

²² Naomi Aoki, Tatemohiko Tatsumi, et.al., "Explainable AI for Government: Does the Type of Explanation Matter to the Accuracy, Fairness, and Trustworthiness of an Algorithmic Decision as Perceived by Those Who Are Affected?", 41 *Government Information Quarterly* 101965 (2024).

²³ "AI and Emerging Technologies in the European Public Sector in 2025", available at: <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/news/ai-and-emerging-technologies-european-public-sector-2025> (last visited on August 24, 2026).

procedures begins to blur. As a result, explanation, documentation and oversight begin to be normal components of lawful governmental decision-making, as opposed to being unusual components of experimental systems.

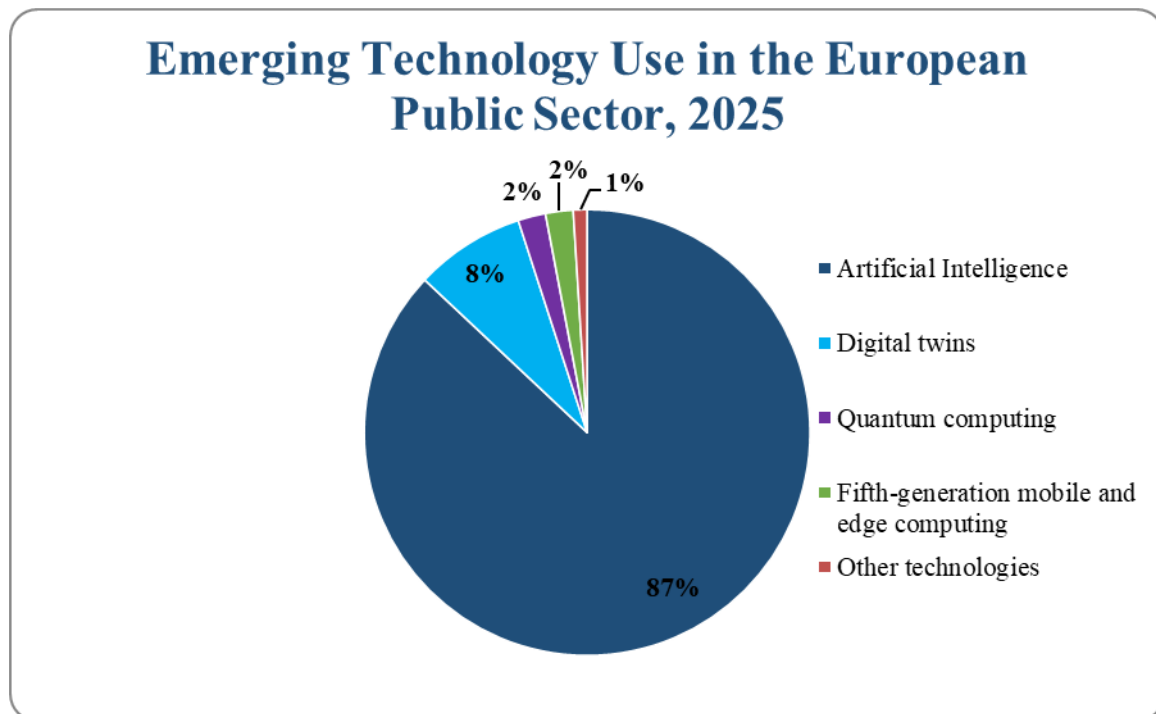


Figure 2. Emerging technology use in the European public sector, 2025. Source: European Commission.

1.4 PROCEDURAL DUE PROCESS AND ADMINISTRATIVE REVIEW IN THE UNITED STATES

There is no single federal statute in the United States that mirrors the Artificial Intelligence Act of the European Union. There are some protections that exist from Sector-specific Litigation, administrative review, and constitutional procedural and substantive due process, and are augmented by executive orders and policies. This system of protection is flexible; however, protections afforded will depend on the interest being protected, what institutional structures are in place, and the context within which the system is inserted.²⁴

1.4.1 Constitutional Procedure and the Risk of Error

Procedural due process requires a fair procedure before government entities infringe on protected interests. In *Goldberg v. Kelly*²⁵, the Supreme Court required that the Department of

²⁴ David Freeman Engstrom and Daniel E. Ho, "Algorithmic Accountability in the Administrative State", 37 *Yale Journal on Regulation* 800 (2020).

²⁵ 397 U.S. 254 (1970).

Welfare had to follow rules for the termination of welfare benefits. An erroneous deprivation of those benefits would have been detrimental and caused the beneficiaries to suffer severe and potentially permanent harm. Automated Decision Systems increase the likelihood this concern will be realized. Executive Branch decisions can occur at a much faster rate. This speed can result in an incorrect data point or assumption being adopted across thousands of cases. In cases involving important benefits or status, notice should identify the legal conclusion as well as the important factual inputs and any critical automated decision-making.

The balancing framework in *Mathews v. Eldridge*²⁶ tends to work better in algorithmic systems, since it takes into account the risk of erroneous deprivation and the potential value of added safeguards. Automation bias, weak human oversight, ill-representative data, proxy variables, and model error all tend to increase this risk. Audit trails, explainable AI, and targeted reconsideration all tend to decrease this risk. Thus, the doctrine tends to lean toward the need for calibrating automation as opposed to an absolute prohibition of automation. Risk of automation should be mitigated even more in high-impact cases, and in cases of a substantial private interest, coupled with a system that poses fatal errors that an average user would not be able to identify.

1.4.2 Opaque Models, Vendor Secrecy and Public Benefits

American litigation tends to uncover proprietary decision-making systems as well. In the case of *Houston Federation of Teachers, Local 2415 v. Houston Independent School District*²⁷, teachers sued over an evaluation system that used a proprietary value-added model, as they argued they could not score their own tests. This problem is not just about employment. A public authority will lose its constitutional obligation and accountability if logic becomes inaccessible as it is vendor-controlled. Trade secrets may justify some closed systems, but government should retain the ability to explain and audit its decision-making process.

Public-benefit litigation demonstrates a related notice problem. A case of particular importance in this context is *K. W. v. Armstrong*²⁸. The United States Court of Appeals for the Ninth Circuit held that appropriate notices must inform benefit recipients of enough information to invalidate the government's action. In the context of an algorithm, a notice that informs the recipient of a consequence, such as a risk score or a reduced service allocation, for example, is insufficient. The notice must explain how the service allocation

²⁶ 424 U.S. 319 (1976).

²⁷ 251 F. Supp. 3d 1168 (S.D. Tex. 2017).

²⁸ 789 F.3d 962 (9th Cir. 2015).

was determined. The focus of the new standard should be on what an individual needs to correct an error, as opposed to the formal disclosure that software was used to make the decision.

1.4.3 Federal Artificial Intelligence Governance and Transparency

The gap in this area of federal policy means that the cumbersome administrative governance systems added by the executive policy significantly reduce agency discretion. For example, Memorandum M-25-21, dated 3 April 2025, was issued by the Office of Management and Budget. This memorandum instructs executive agencies to repair the balance between the use of Artificial Intelligence in the public sector and civil rights, civil liberties, and privacy protection.²⁹ This memorandum establishes the requirements for the use of high impact Artificial Intelligence and the inventories and governance of Artificial Intelligence. The memorandum shifts the risk management burden to the agency inside the organization and creates a record on leadership. However, the policy does not create an enforceable right. The strongest contribution of the policy to due process is the creation of records that establish risk management.

The data that the federal government provides shows how big this challenge is when it comes to scale and transparency. The United States Government Accountability Office found that for fiscal year 2022, 20 of the government's agencies demonstrated the use of 1,241 existing and planned AI technology. This data is disclosed as shown in Figure 3.³⁰ These numbers are historical baselines and not a planned inventory of 2026. The Government Accountability Office also noted limitations to the reporting. However, legitimate confidentiality cannot prevent accountability and oversight, nor can it prevent the disclosure from occurring to the intended parties who may be affected by an automated output that contributes to government action.

²⁹ Office of Management and Budget, "Memorandum M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust" (April 3, 2025).

³⁰ United States Government Accountability Office, "Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements" (GAO-24-105980, December, 2023).

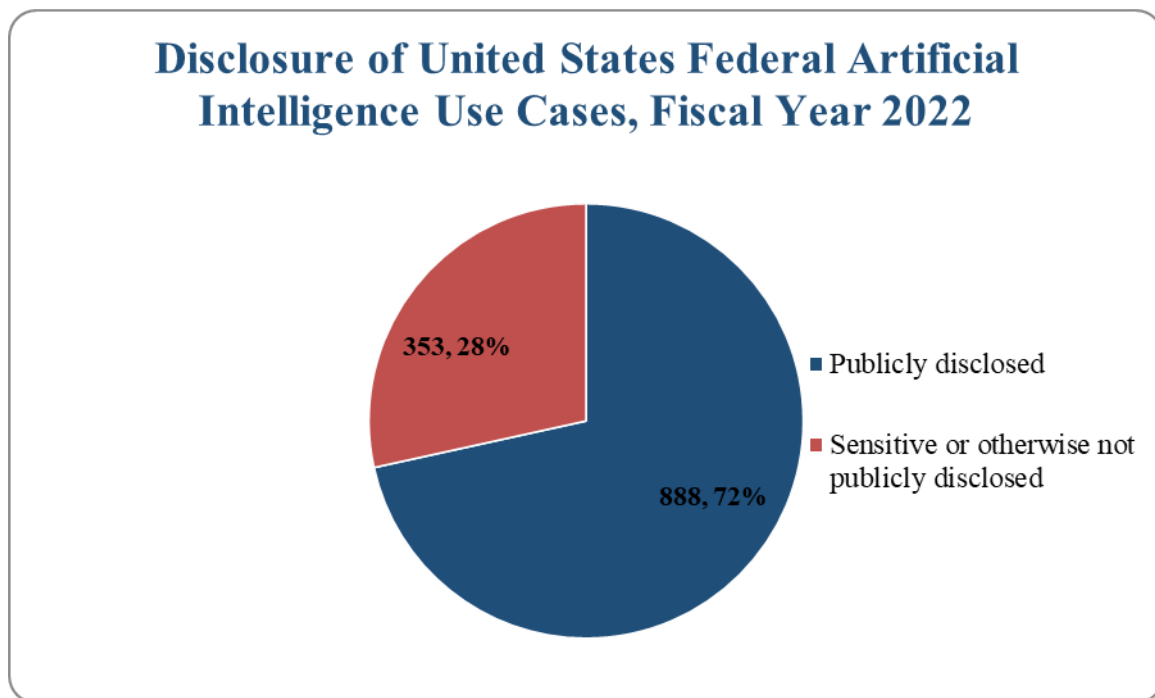


Figure 3. *Disclosure of United States federal Artificial Intelligence use cases, fiscal year 2022. Source: United States Government Accountability Office.*

1.5 COMPARATIVE DUE PROCESS AND AN INDIAN REFORM MODEL

Looking at different systems and structures, we also see a significant amount of convergence. Every system demonstrates the importance of public accountability in the ability to understand the reasoning, review, and correct the actions. The main divergence is the focus of regulation. The European Union uses a continual focus on lifecycle regulation. The United States prefers procedural regulation, and India has a broad standard of the Constitution and evolving support.³¹

1.5.1 From Formal Transparency to Effective Contestability

The first lesson in comparison is that transparency should be defined in terms of its legal function. In informational capitalism, Julie E. Cohen describes how institutional power is shaped by the power to define, construct, and control information and its related infrastructures and legal domains. Therefore, in public administration, disclosure is important as it re-distributes the ability to challenge a decision.³² Even a detailed model card may be valuable to an auditor, but to a pensioner challenging a decision, it may be completely worthless. Nevertheless, a brief individual explanation that identifies the important data and

³¹ Karen Yeung and Martin Lodge (eds.), *Algorithmic Regulation 1* (Oxford University Press, Oxford, 1st edn., 2019).

³² Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism 5* (Oxford University Press, New York, 1st edn., 2019).

criteria and the path by which the decision may be challenged is of great value. Indian law should differentiate system-level transparency for oversight from the rationale of the decision for the person affected.

The second lesson is that reviewability should be designed into the system. Jennifer Cobbe and Jatinder Singh support the right to review by proposing automated decision systems that preserve the conditions necessary for review. Indian public bodies should record model version and inputs, as well as the output, human interventions, overrides, and corrections for each model version.³³ Although these records would not need to be given to each and every claimant, they must allow the authority, the auditor, and the court to reconstruct the legally significant pathway. Otherwise, judicial review will be deferential simply because the necessary evidence is lacking.

1.5.2 Meaningful Human Review and Graduated Safeguards

Human oversight should be substantive rather than ceremonial. A reviewer who is not able to deviate from an algorithm, only receives its score, or is expected to review cases so quickly that they cannot investigate anomalies provides little additional protection. Meaningful human reconsideration requires access to the relevant record, an understanding of the system's limitations, and the ability to change the outcome. All these should be provided prior to irrevocable or severely challenging decisions in high-risk domains. More dangerous tools can demand more robust protections, and less dangerous tools can demand less. More dangerous tools should grant more oversight, and less dangerous tools can grant less. This approach allows automation to be embraced for more routine, reversible, and lower risk tasks.³⁴

Public acceptance is not a substitute for legality; however public perception of fairness is relevant for the legitimacy of an institution. The studies of Tessa Haesevoets, Bram Verschuere, Ruben Van Severen and Arne Roets focus on the citizen's perception of artificial intelligence in public-sector decision making. In administrative law, procedures indicate whether the government views the individual as a participant or whether the government treats the individual as an object of classification.³⁵ Therefore, human review should be evident, and human review should be accessible. The notification should indicate the constituency that is authorized to review the decision and should indicate the necessary

³³ Jennifer Cobbe and Jatinder Singh, "Reviewable Automated Decision-Making", 39 *Computer Law & Security Review* 105475 (2020).

³⁴ Ben Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 45 *Computer Law & Security Review* 105681 (2022).

³⁵ Tessa Haesevoets, Bram Verschuere, et.al., "How Do Citizens Perceive the Use of Artificial Intelligence in Public Sector Decisions?", 41 *Government Information Quarterly* 101906 (2024).

evidentiary material, the time allowed for the submission, and the determination of whether review will delay the implementation of a decision with serious adverse impact.

1.5.3 A Public-Law Framework for High-Impact Systems in India

The rapid advancement of governmental AI requires India to create a formal or legally binding executive framework for high-impact governmental AI, rather than attempting to regulate every type of AI used by the government the same way. We would consider a system as high-impact when the output materially impacts or constrains legal decisions regarding important rights, public benefits, the right to work or study, access to healthcare, etc. The label given to a system should not be used as a determinant in making the high-impact classification. Agencies should not be able to avoid safeguards by putting a nominal check of human approval, while keeping it an administrative system. This definition would maintain the flexibility of administrative systems and would not allow agencies to avoid safeguards.³⁶

For high-impact systems, the assessing authority would be required to complete an Algorithmic Impact Assessment which must include the legal basis, the purpose, impacted groups, data sources, known issues, the validation processes, testing for discrimination, security, oversight, and the means through which the adverse impact can be remedied. This assessment must address less intrusive alternatives and must explain the design in the context of the administrative objective. This assessment must be published, but sensitive security information may be omitted. Procurement contracts must ensure the government has the right to audit the models and that the auditing records are retained. It must not be the case that a vendor maintains secrecy that inhibits the government's ability to fulfill its legal obligations.³⁷

After the employee receives the adverse decision that was based on algorithms, the employee must receive an explanation from the employee regarding the decision and the factors that the automated system weighed to the employee's detriment. The employee must also have the right to challenge the data and appear before a decision-maker. Finally, the state employee must document all the information so that an administrative hearing and court of law can review the process. When the state employee defends the process by the administrative law, courts will examine the system and if the employee complied with the requirements of ordinary legal decision making, the system will be considered reasonable, non-arbitrary, and

³⁶ Office of the Principal Scientific Adviser to the Government of India, *"Strengthening AI Governance Through Techno-Legal Framework"* (January, 2026).

³⁷ AI Now Institute, *"Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability"* (April, 2018).

fair. This proposal aims to shield employees from the law of algorithms and ensures that state employees must justify the decisions, even with technological systems, that can be opaque.³⁸

1.6 CONCLUSION

Algorithmic governance does not cancel administrative law; it shifts the circumstance under which administrative law is applicable. The primary question throughout the three jurisdictions is whether computational assistance retains meaningful notice, reasons, and human judgment, and review and not whether a human official is situated in the formal chain.³⁹

This analysis illustrates different approaches that share common public law issues. The European Union integrates procedural safeguards into its data protection and Artificial Intelligence legislation. The United States uses constitutional balancing, administrative review, and executive branch governance. These approaches create substantial protections in some situations but leave other institutional protections incomplete. India has broad constitutional protections in fairness, non-arbitrariness, privacy, and proportionality, along with a developing policy framework. India's main challenge, therefore, is not the absence of doctrine, but rather the lack of transformation of doctrine into practical implication. Without supporting documentation, explanation, review, and audit duties, principles of constitutionality and procedural fairness may come into force only after thousands of decisions have been made.⁴⁰

The Indian approach to algorithmic due process should remain grounded in general public law. High impact systems should be implemented with lawful authority, limited and appropriate use of data, assessment prior to implementation, system accountability including the right to meaningful review, and sufficient judicial review. The safeguards do not require publication of source code or prohibit beneficial automation. The purpose of the safeguards is to avoid computational systems from replacing existing substantive protections of the administrative process. The degree of justification, contestability, and accountability of public power remains the standard for constitutional review. Technology may change the methods by which decisions are made, but it cannot relieve the government from the obligation to justify and defend decisions that affect the interests of individuals.⁴¹

³⁸ Ryan Calo and Danielle Keats Citron, "The Automated Administrative State: A Crisis of Legitimacy", 70 *Emory Law Journal* 797 (2021).

³⁹ Danielle Keats Citron, "Technological Due Process", 85 *Washington University Law Review* 1249 (2008).

⁴⁰ Cary Coglianese and David Lehr, "Transparency and Algorithmic Governance", 71 *Administrative Law Review* 1 (2019).

⁴¹ Divij Joshi, "AI Governance in India - Law, Policy and Political Economy", 10 *Communication Research and Practice* 328 (2024).

1.6.1 SUGGESTIONS

This analysis will help to develop a project to make public sector automation in India more legally accountable and institutionally reliable.

1. Define high-impact systems: Automation decisions should be binding if they impact a person's rights, benefits, or access to services. The classification should be based on real world impact and not based on how an agency characterizes their advisory system.
2. Mandate impact assessments: Have public authorities record legal basis and documentation of purpose and sources, affected groups, validation, discrimination risks, and human oversight and remedies prior to deployment. Publish a sanitized version to high-impact systems.
3. Require algorithmic notice: Notify affected individuals when automated processing materially impacts an adverse administrative decision. Notifications should indicate the decision and data that support the decision, not just that software was utilized.
4. Guarantee human reconsideration: Include an authorized official's review to disregard the automated recommendation and alter the result. Significant adverse decisions should not be made final until reviewed after a considerable time.
5. Preserve auditable records: For each significant decision, record the version of the model, material inputs, the output, interventions and corrections by humans. Records should enable review by the department and an independent audit at a later date, as well as scrutiny by a justice investigator without needing reconstruction.
6. Strengthen procurement clauses: Include audit access, technical documentation, data provenance, and the ability to receive notice with explanation for model changes in government contracts. Government contract procurement should not be restricted due to commercial secrecy. Government contract purchasing authorities should not be unconstitutional or in violation of administrative law.
7. Build independent assurance: Create technically competent audit functions alongside or within sectoral regulators. At regular intervals, these audit functions are designed to test accuracy, discrimination, security, privacy, model drift and the overall impact of human oversight.
8. Create fallback procedures: Ensure that the unavailability of a public service does not occur due to authentication failure, data mismatch, or output with low confidence. Departments are expected to create parallel means of verification and offer rapid corrections.
9. Publish a system register: Create and maintain a searchable database containing the purposes, responsible authority, legal basis, and risk classification of governmental AI

systems. Inform users when a material change happens to the function, model, or data source for a system.

10. Standardise judicial review: When reviewing the statutory basis and other inputs, courts should look for a rational connection and test for proportionality and explanation. Human review and the reliability of the evidence should also be considered. A consistent review framework should prevent unprincipled deference even with complex technologies.

BIBLIOGRAPHY

Books

1. Cohen, J. E., *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, New York, 1st edn., 2019).
2. Eubanks, V., *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press, New York, 1st edn., 2018).
3. Hildebrandt, M., *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, Cheltenham, 1st edn., 2015).
4. Pasquale, F., *Secret Algorithms That Control Money and Information* (Harvard University Press, Cambridge, MA, 1st edn., 2015).
5. Yeung, K. and (eds.), M. L., *Algorithmic Regulation* (Oxford University Press, Oxford, 1st edn., 2019).

Statutes

6. The Charter of Fundamental Rights of the European Union, 2012 (2012/C 326/02)
7. The Constitution of India, 1950
8. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
9. The Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 (Regulation (EU) 2016/679)
10. The Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act), 2024 (Regulation (EU) 2024/1689)

Reports

11. Aayog, N. I. T. I., "Responsible AI #AIForAll: Approach Document for India, Part 2: Operationalizing Principles for Responsible AI" (August, 2021).
12. AI Now Institute, "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability" (April, 2018).
13. Report of Government of India, Ministry of Electronics and Information Technology: India AI Governance Guidelines.

14. Management, O. O. and Budget, "Memorandum M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust" (April 3, 2025).
15. Report of Office of the Principal Scientific Adviser to the Government of India: Strengthening AI Governance Through Techno-Legal Framework.

Articles

16. Aoki, N., Tatsumi, T., et al., "Explainable AI for Government: Does the Type of Explanation Matter to the Accuracy, Fairness, and Trustworthiness of an Algorithmic Decision as Perceived by Those Who Are Affected?", 41 Government Information Quarterly 101965 (2024).
17. Calo, R. and Citron, D. K., "The Automated Administrative State: A Crisis of Legitimacy", 70 Emory Law Journal 797 (2021).
18. Citron, D. K., "Technological Due Process", 85 Washington University Law Review 1249 (2008).
19. Cobbe, J. and Singh, J., "Reviewable Automated Decision-Making", 39 Computer Law & Security Review 105475 (2020).
20. Coglianese, C. and Lehr, D., "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era", 105 Georgetown Law Journal 1147 (2017).
21. Coglianese, C. and Lehr, D., "Transparency and Algorithmic Governance", 71 Administrative Law Review 1 (2019).
22. Engstrom, D. F. and Ho, D. E., "Algorithmic Accountability in the Administrative State", 37 Yale Journal on Regulation 800 (2020).
23. Geburczyk, F., "Automated Administrative Decision-Making under the Influence of the GDPR: Early Reflections and Upcoming Challenges", 41 Computer Law & Security Review 105538 (2021).
24. Green, B., "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 45 Computer Law & Security Review 105681 (2022).
25. Haesevoets, T., Verschuere, B., et al., "How Do Citizens Perceive the Use of Artificial Intelligence in Public Sector Decisions?", 41 Government Information Quarterly 101906 (2024).
26. Janssen, M. and Kuk, G., "The Challenges and Limits of Big Data Algorithms in Technocratic Governance", 33 Government Information Quarterly 371 (2016).
27. Joshi, D., "AI Governance in India - Law, Policy and Political Economy", 10 Communication Research and Practice 328 (2024).

Websites

28. <https://digital-strategy.ec.europa.eu/en/policies/enforcement-ai-act>
29. <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/news/ai-and-emerging-technologies-european-public-sector-2025>
30. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2291062&lang=1®=3>