INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

BEYOND DATA PROTECTION: CONSTITUTIONAL ACCOUNTABILITY AND THE REGULATION OF ARTIFICIAL INTELLIGENCE IN INDIAN PUBLIC ADMINISTRATION — A COMPARATIVE STUDY WITH THE EUROPEAN UNION'S GDPR

AUTHORED BY - YASHWARDHAN SINGH TOMAR
Institution – Jagran Lakecity University
Course – B.B.A. LL.B. (Hons.)

Abstract

The increasing integration of artificial intelligence (AI) into public administration is transforming the manner in which governments exercise administrative authority, distribute public resources and deliver essential services. Predictive policing, automated welfare administration, biometric identification, algorithmic risk assessment and AI-assisted decision-making promise greater administrative efficiency; nevertheless, they also create substantial concerns regarding privacy, equality, procedural fairness, transparency and institutional accountability. These concerns become particularly serious when algorithmic systems influence decisions affecting an individual's legal status, livelihood or access to public entitlements. Although India has developed a constitutional jurisprudence on privacy and enacted the Digital Personal Data Protection Act, 2023, its approach to AI governance remains distributed across general legislation, sectoral regulation and policy instruments. The European Union, by contrast, has developed a more structured data-protection regime through the General Data Protection Regulation (GDPR), supplemented by the AI Act's risk-based regulatory obligations.

This paper examines whether India's existing legal framework adequately addresses the challenges created by AI-assisted public administration. Adopting a doctrinal and comparative methodology, it analyses the constitutional foundations of privacy and equality in India, the statutory framework under the Digital Personal Data Protection Act, 2023, the India AI Governance Guidelines, 2025, and the relevant provisions of the GDPR. It further considers the relationship between data protection and the broader regulation of algorithmic decision-making. The paper argues that data protection, although indispensable, cannot independently

ISSN: 2582-6433

guarantee lawful and accountable public-sector AI. The principal regulatory gap lies in the absence of a sufficiently developed, enforceable framework governing the use of algorithmic systems in the exercise of public power. Drawing on European regulatory experience while accounting for India's constitutional structure and administrative realities, the paper proposes a rights-based and risk-sensitive framework incorporating algorithmic impact assessments, meaningful human oversight, reasoned decisions, independent auditing, public transparency and accessible remedies. It concludes that the legitimacy of AI-enabled governance must be assessed not merely by administrative efficiency, but by its compatibility with constitutional democracy and the rule of law.

Keywords: Artificial Intelligence; Public Administration; Indian Constitutional Law; Digital Personal Data Protection Act, 2023; General Data Protection Regulation; Algorithmic Accountability; Automated Decision-Making; Right to Privacy; Administrative Law; AI Governance.

1. Introduction

Artificial intelligence has increasingly moved beyond the domain of technological experimentation to become an instrument through which governments organise, administer and exercise public authority. Contemporary public institutions employ algorithmic systems to analyse information, identify patterns, allocate resources and assist administrative decision-making. Applications range from predictive policing and biometric identification to automated welfare administration, healthcare management, urban planning and judicial assistance. These developments have altered the relationship between the citizen and the administrative state. Decisions that were traditionally made through human assessment and institutional discretion may now be informed, ranked or, in certain circumstances, substantially determined by computational systems.

The adoption of AI in public administration is frequently justified by reference to efficiency, consistency, cost reduction and improved service delivery. Such objectives are not inherently incompatible with constitutional governance. Indeed, properly designed technological systems may improve the accessibility of public services and assist governments in addressing complex administrative problems. The difficulty arises when efficiency becomes the dominant measure of administrative success, while the legal and social consequences of automated decisions receive insufficient attention. A system that processes applications rapidly but systematically excludes eligible beneficiaries cannot be considered an effective instrument of public

ISSN: 2582-6433

administration. Similarly, a predictive policing tool that reproduces historical patterns of discriminatory enforcement may increase operational efficiency while undermining the constitutional commitment to equality.

The distinctive concern associated with AI in government is therefore not simply that algorithms may make mistakes. It is that their outputs can influence the exercise of public power without the transparency, accountability and procedural safeguards traditionally expected of administrative authorities. Where a welfare application is rejected, a person is classified as a security risk or an individual is subjected to heightened surveillance, the affected person must be able to understand the basis of the decision and pursue an effective remedy. The use of technology cannot, by itself, displace these requirements.

India's constitutional framework provides an important starting point for this inquiry. Article 14 guarantees equality before the law and equal protection of the laws, while Article 21 protects life and personal liberty. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v Union of India* established a constitutional foundation for examining state practices involving the collection, processing and use of personal information. These constitutional guarantees are particularly relevant where AI systems facilitate large-scale profiling, biometric surveillance or automated administrative classification.[1]

At the statutory level, the Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's principal legislative framework for digital personal data. It regulates the processing of digital personal data and establishes obligations for Data Fiduciaries alongside rights for Data Principals. However, data protection and AI governance are not identical regulatory concerns. A system may process personal data in accordance with applicable data protection requirements and nevertheless produce discriminatory outcomes, operate through inadequately reasoned administrative procedures or undermine the ability of an individual to challenge a public decision. The legal question consequently extends beyond whether data has been processed lawfully. It also concerns whether the public authority's decision-making process is constitutionally and administratively legitimate.

The European Union offers a useful comparative framework. The GDPR establishes a comprehensive regime governing personal data processing, including transparency obligations, accountability requirements, data protection impact assessments and restrictions on certain forms of solely automated decision-making. The EU AI Act, Regulation (EU) 2024/1689, supplements this framework through risk-based obligations applicable to specified AI systems. The European experience is therefore instructive not because it can be transplanted wholesale into India, but because it demonstrates how data protection, AI-specific obligations and

ISSN: 2582-6433

fundamental rights assessments can operate as complementary elements of a regulatory system. This paper contends that India should move towards a more explicit framework for algorithmic accountability in public administration. Such a framework should preserve technological innovation while ensuring that public authorities remain legally answerable for decisions made with the assistance of AI. The central proposition is that the legitimacy of AI-enabled public administration depends on the preservation of constitutional rights, procedural fairness and effective institutional accountability, rather than on technological efficiency alone.

2. Research Problem, Objectives and Questions

2.1 Research problem

India's legal framework addresses several dimensions of AI-related harm through constitutional guarantees, data protection legislation, information technology law and sector-specific regulation. Nevertheless, these legal instruments do not necessarily provide a coherent answer to the distinct problems created when AI systems influence administrative decisions. In particular, questions concerning algorithmic explainability, discriminatory outputs, human reconsideration, public-sector impact assessments and responsibility for automated decisions remain insufficiently integrated into a single enforceable framework.

The problem is especially significant in welfare administration, law enforcement and other areas in which an incorrect algorithmic assessment may have serious consequences for individual rights and entitlements. The absence of a clear and accessible mechanism for challenging such decisions may render existing legal protections difficult to exercise in practice.

2.2 Objectives

The paper has four principal objectives:

1. To examine the constitutional and statutory foundations governing the use of AI in Indian public administration.
2. To analyse the extent to which the DPDP Act, 2023 addresses the risks associated with algorithmic decision-making.
3. To compare India's data protection framework with the GDPR, particularly in relation to automated decisions, transparency, accountability and impact assessments.
4. To propose a rights-based regulatory framework for AI-assisted public administration in India.

ISSN: 2582-6433

2.3 Research questions

The study addresses the following questions:

I. To what extent do Articles 14 and 21 of the Constitution of India constrain the use of AI in public administration?

II. Does the DPDP Act, 2023 provide adequate safeguards against the risks arising from automated and algorithmically assisted administrative decisions?

III. How does the Indian data protection framework differ from the GDPR in its treatment of automated decision-making and individual rights?

IV. What institutional and procedural safeguards are necessary to ensure that AI-assisted government decisions remain transparent, reviewable and constitutionally legitimate?

3. Research Methodology and Scope

This study adopts a doctrinal and comparative legal research methodology. It examines constitutional provisions, statutory instruments, judicial decisions, regulatory frameworks and relevant academic literature concerning AI governance and data protection. The Indian legal analysis primarily considers Articles 14 and 21 of the Constitution, the Digital Personal Data Protection Act, 2023, the India AI Governance Guidelines, 2025, and relevant judicial developments. The comparative analysis focuses on Regulation (EU) 2016/679, commonly known as the GDPR, and draws on the EU AI Act where necessary to distinguish general data protection from AI-specific regulation.

The study is qualitative and analytical rather than empirical. It does not claim to measure the actual frequency of algorithmic discrimination in Indian public institutions or to provide a statistical assessment of the effectiveness of existing safeguards. Its purpose is to identify legal and institutional gaps through an examination of applicable norms and comparative regulatory experience.

The legal position is considered as at 11 November 2026. Particular attention is paid to the phased commencement of the DPDP Act and the DPDP Rules, 2025. This temporal qualification is necessary because enactment, notification and commencement are distinct legal events. The analysis does not assume that every provision of the DPDP Act is already operative merely because the Act and Rules have been notified.

ISSN: 2582-6433

4. Artificial Intelligence and the Transformation of Public Administration

4.1 From administrative discretion to algorithmically assisted governance

Traditional administrative decision-making generally involves the collection of relevant information, consideration of applicable legal standards and the exercise of discretion by an authorised official. AI changes this process by introducing systems capable of processing large datasets, identifying correlations and generating recommendations or classifications. Depending on the design and institutional arrangements, an AI system may operate as a decision-support instrument, a screening mechanism or a significant determinant of the eventual administrative outcome.

This distinction is legally important. An AI system that assists an official in organising documents does not necessarily create the same rights-related concerns as a system that assigns risk scores to individuals or determines eligibility for public benefits. The legal significance of AI therefore depends not only on its technical characteristics but also on the function it performs and the consequences of its use.

Administrative authorities cannot avoid legal responsibility merely because a decision is generated through a technological process. Where a public authority adopts an algorithmic recommendation as the basis of its action, the resulting decision remains attributable to the exercise of public authority. The use of an external developer or private contractor does not transform a public function into an area free from constitutional and administrative scrutiny.

4.2 Algorithmic bias and the reproduction of inequality

Algorithmic bias arises when an AI system produces systematically unfair outcomes, whether because of unrepresentative training data, inappropriate variables, flawed assumptions or the context in which the system is deployed. The problem is particularly serious where historical data reflects existing patterns of social disadvantage.

For example, a predictive policing model trained on historical arrest records may reproduce geographical patterns of intensive policing. The model may then identify the same areas as requiring greater police attention, generating a feedback loop in which historical enforcement patterns influence future enforcement decisions. The resulting prediction may appear statistically objective even though it reflects institutional practices that warrant independent scrutiny.

The COMPAS controversy in the United States illustrates the difficulty of relying on algorithmic risk assessments in criminal justice. The ProPublica investigation raised concerns about racial disparities in the system's error rates, while subsequent academic work examined

ISSN: 2582-6433

the competing statistical definitions of fairness. The wider lesson is that predictive accuracy and legal fairness are not interchangeable. A system may produce statistically useful predictions while still creating unjustified burdens for particular groups.

In the Indian context, similar concerns may arise in recruitment, welfare distribution, policing and public resource allocation. Article 14 requires that state action comply with constitutional standards of equality and non-arbitrariness. An algorithmic classification cannot be treated as legally neutral merely because it is generated by software.

4.3 Transparency, explainability and procedural fairness

AI systems may produce outputs that are difficult for affected individuals and public officials to interpret. This problem is commonly described as algorithmic opacity or the black-box problem. It becomes a legal concern when the reasons for an administrative decision cannot be meaningfully examined.

A person whose application for a public benefit has been rejected should not be left with the unexplained statement that a computer system has determined ineligibility. The person must have a meaningful opportunity to understand the relevant grounds, identify inaccuracies and pursue available remedies.

Transparency in this context should not be reduced to the publication of technical documentation. The information provided must be appropriate to its intended audience. Regulators may require technical access to model documentation, whereas an affected individual ordinarily requires an intelligible explanation of the material reasons for an adverse decision.

The principles of natural justice and reasoned administrative decision-making therefore assume renewed significance in algorithmic governance. AI may assist administrative authorities, but it should not become a mechanism through which procedural fairness is displaced.

5. Constitutional Foundations of AI Governance in India

5.1 Article 14: equality and non-arbitrariness

Article 14 is central to the regulation of AI-assisted public administration because it constrains arbitrary state action and requires equal protection of the laws. Its relevance extends beyond overt discrimination. It also raises questions about the rationality, consistency and fairness of administrative classifications.

Where an algorithm determines the priority of welfare applications, identifies individuals for investigation or influences the allocation of public resources, the authority must be able to

ISSN: 2582-6433

justify the criteria employed. A classification based on inaccurate, irrelevant or discriminatory variables may raise constitutional concerns even if the system is functioning as designed.

The difficulty is that algorithmic systems can conceal the assumptions underlying administrative classifications. A model may use variables that appear neutral but operate as proxies for caste, religion, economic vulnerability or geographical disadvantage. The legal assessment must therefore examine the practical effects of the system rather than relying solely on the stated neutrality of its inputs.

Article 14 should consequently inform the design, procurement, deployment and review of public-sector AI systems. Where an algorithm materially influences an adverse administrative decision, the public authority should be able to demonstrate that the decision rests on legally relevant considerations and is not arbitrary or discriminatory.

5.2 Article 21: privacy, dignity and personal liberty

The constitutional right to privacy recognised in *Puttaswamy* provides a fundamental basis for scrutinising state use of personal information. The Supreme Court located privacy within the protection of life and personal liberty under Article 21 and recognised its connection with dignity and individual autonomy.

AI systems can intensify privacy concerns because they enable the aggregation, analysis and inference of information at a scale that may not be possible through conventional administrative processes. Facial recognition, biometric identification, predictive profiling and the combination of government databases can create detailed profiles of individuals and communities.

The proportionality principle is particularly relevant. A restriction on privacy must have a lawful basis and pursue a legitimate objective, while satisfying the applicable requirements of suitability, necessity and balancing. The state cannot establish the constitutional legitimacy of intrusive AI surveillance merely by asserting that the technology may improve public safety or administrative efficiency.

The decision in *K.S. Puttaswamy (Aadhaar-5J) v Union of India* further demonstrates the importance of proportionality in examining state use of identity infrastructure. Although the judgment concerned the Aadhaar framework rather than AI regulation as such, its reasoning is relevant to technological systems involving identification, authentication and the processing of personal information.

5.3 Natural justice and the right to challenge administrative decisions

The principles of natural justice require fair procedures where administrative action adversely

ISSN: 2582-6433

affects individual interests. Their application to algorithmic decision-making raises questions about notice, disclosure of relevant reasons, opportunities to respond and meaningful reconsideration.

Consider a hypothetical system that flags a welfare beneficiary as ineligible because of an incorrect data match. If the individual receives no intelligible explanation and has no practical opportunity to correct the underlying information, the administrative process may become procedurally unfair.

Human review is therefore important, but it must be substantive rather than ceremonial. An official who merely approves an algorithmic recommendation without examining its basis does not provide meaningful oversight. Effective review requires sufficient authority, relevant information and the practical ability to depart from the system's recommendation.

5.4 The relationship between constitutional review and statutory data protection

Constitutional guarantees and data protection legislation perform related but distinct functions. Data protection law regulates the processing of personal information, while constitutional and administrative law govern the legality of state action and the exercise of public power.

A public authority may comply with certain data-processing obligations and still act arbitrarily in the way it uses an algorithmic output. Conversely, an administrative decision may raise privacy concerns even where the ultimate decision is not based solely on automated processing.

The regulatory framework must therefore preserve the independent operation of constitutional review. Data protection compliance should be treated as one component of lawful AI deployment, not as conclusive proof that an administrative decision is constitutionally valid.

6. India's Statutory and Policy Framework for AI Governance

6.1 The Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 establishes a statutory framework for processing digital personal data in India. It recognises the interests of individuals in protecting their personal data while permitting processing for lawful purposes. The Act uses the concepts of Data Fiduciary and Data Principal to allocate responsibilities and rights within the data-processing relationship.

The Act is relevant to public-sector AI because government systems frequently rely on personal information to identify individuals, assess eligibility, detect anomalies and deliver services. Its principles and obligations may therefore apply to AI systems to the extent that their operations involve digital personal data within the Act's scope.

The Act's principal features include obligations relating to lawful processing, notice and

ISSN: 2582-6433

consent, certain legitimate uses, security safeguards, data breach obligations, individual rights and the institutional role of the Data Protection Board of India. These provisions provide an important foundation for regulating the data lifecycle associated with AI systems.

Nevertheless, the Act is not a comprehensive AI statute. It does not establish a general system of algorithmic fairness assessments for all public-sector AI applications, nor does it create a universal right to challenge every decision influenced by an algorithm. Its primary regulatory focus is the processing of digital personal data.

This distinction has practical consequences. An AI system may produce discriminatory outcomes through the use of variables or statistical correlations even where the processing of personal data is otherwise lawful. Similarly, an automated public decision may be procedurally unfair without necessarily involving a breach of a data protection obligation. Additional safeguards are therefore required to address the full range of algorithmic harms.

6.2 Government processing and statutory exemptions

The treatment of government processing under the DPDP Act requires particular attention. Section 7 recognises specified uses of personal data that may be undertaken without relying on consent, subject to the conditions prescribed by the Act. Section 17 provides for exemptions in specified circumstances.

These provisions must be understood within the statutory scheme rather than treated as a general authorisation for unrestricted state data processing. Nevertheless, exemptions and government processing powers require careful scrutiny because public-sector AI may involve extensive datasets and affect individuals who have limited bargaining power or no realistic alternative to interacting with government systems.

The constitutional requirements of legality, legitimate purpose and proportionality remain important. Statutory permission to process personal data should not be confused with an unrestricted power to deploy any algorithmic system for any administrative objective.

6.3 Phased commencement of the DPDP Act and Rules

A significant temporal qualification is necessary. Although the DPDP Act received presidential assent in August 2023 and the Digital Personal Data Protection Rules were notified in November 2025, their commencement was structured in phases.

The commencement notification, G.S.R. 843(E), dated 13 November 2025, brought specified institutional and preliminary provisions into force immediately, provided for certain provisions to commence after one year and scheduled the principal group of substantive provisions for

ISSN: 2582-6433

commencement 18 months after publication. The Rules, notified through G.S.R. 846(E), also follow a phased commencement arrangement.

Accordingly, as at 11 November 2026, the principal substantive obligations and individual rights under the Act are not yet fully in force. The principal group is scheduled to commence in May 2027, while certain specified provisions are scheduled for November 2026. This distinction between enactment, notification and commencement is essential to an accurate statement of Indian law.

The transitional period also provides an opportunity to develop complementary safeguards for AI-assisted public administration before the full substantive framework becomes operative.

6.4 India AI Governance Guidelines, 2025

The India AI Governance Guidelines, released by the Ministry of Electronics and Information Technology in November 2025, represent an important development in India's policy approach. The Guidelines seek to promote safe, responsible and inclusive AI adoption through a principle-based and risk-sensitive governance framework.

Their significance lies in recognising that AI risks must be addressed through coordinated institutional action and existing legal and regulatory structures. They emphasise responsible deployment, mitigation of harms and the participation of relevant sectoral institutions.

However, the Guidelines are policy guidance rather than a comprehensive statutory AI code. They do not, by themselves, create a general statutory right to an explanation of an algorithmic administrative decision or a universal statutory requirement for independent algorithmic audits. Their practical effect therefore depends substantially on implementation through existing legal powers, regulatory action and institutional practices.

This approach offers flexibility and may be appropriate during a period of rapid technological development. Its limitation is that principle-based guidance cannot always provide the certainty, enforceability and remedies associated with legislation.

6.5 Existing legal instruments and sectoral regulation

AI systems may also intersect with other areas of Indian law, including the Information Technology Act, 2000, sector-specific regulatory requirements, constitutional remedies and administrative law. The legal framework applicable to a particular AI system will depend on its purpose, the nature of the data involved, the identity of the deploying institution and the consequences of its use.

The resulting regulatory structure is therefore plural rather than entirely absent. The difficulty

ISSN: 2582-6433

is that existing legal instruments were not necessarily designed to address the specific characteristics of algorithmic public decision-making. A coherent framework must connect these existing laws with more explicit requirements for transparency, risk assessment, human oversight and redress.

7. Comparative Analysis: India's Data Protection Framework and the European GDPR

7.1 The GDPR as a comprehensive data protection framework

Regulation (EU) 2016/679, the General Data Protection Regulation, establishes a comprehensive legal regime governing the processing of personal data within its territorial scope. It is based on principles including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.

The GDPR is particularly relevant to AI governance because many AI systems rely on personal data for training, profiling, prediction and decision support. Its requirements apply to personal data processing regardless of whether the processing is undertaken through conventional databases or advanced algorithmic systems.

The GDPR should not, however, be mistaken for a complete AI regulatory framework. Its central concern is the protection of personal data and the rights of data subjects. The EU AI Act separately addresses the risks associated with specified AI systems, including certain high-risk applications.

7.2 Principles of processing: India and the GDPR

Both the DPDP Act and GDPR seek to regulate the processing of personal data through statutory obligations. Their approaches, however, differ in structure and detail.

The GDPR expressly establishes a broad set of data protection principles in Article 5. These include purpose limitation, data minimisation, accuracy, storage limitation and accountability. Article 6 provides the legal bases for processing, while Article 9 imposes additional restrictions on the processing of special categories of personal data.

The DPDP Act adopts its own statutory structure, including provisions concerning notice, consent, specified legitimate uses, Data Fiduciary obligations and individual rights. It does not reproduce the GDPR's full architecture or its precise distinction between ordinary personal data and special categories of personal data.

This difference is important for AI systems that use sensitive information or infer

ISSN: 2582-6433

characteristics about individuals. The GDPR's differentiated treatment of special categories provides a more explicit statutory structure for certain sensitive forms of processing. India's framework instead relies on its own statutory categories, obligations and exemptions.

7.3 Automated decision-making and profiling

One of the most significant points of comparison concerns Article 22 of the GDPR.

Article 22 provides a right not to be subject to a decision based solely on automated processing, including profiling, where the decision produces legal effects concerning the individual or similarly significantly affects that individual. The provision recognises exceptions, including where the decision is necessary for a contract, authorised by Union or Member State law with suitable safeguards, or based on explicit consent. In specified cases, safeguards include human intervention, the opportunity to express a point of view and the ability to contest the decision.

The significance of Article 22 is that it addresses a particular category of automated decision-making rather than merely regulating the collection and storage of data. It recognises that certain decisions may have serious consequences for individuals and that safeguards are required when those decisions are made solely through automated processing.

The DPDP Act does not contain an equivalent general provision establishing a comparable right not to be subject to solely automated decisions producing legal or similarly significant effects. the principally concern personal data processing. Consequently, an individual affected by an AI-assisted government decision may need to rely on other applicable statutory provisions, constitutional remedies and administrative law principles rather than a directly equivalent provision to GDPR Article 22.

This is a material difference. The Indian framework may regulate the personal data used by an algorithm without comprehensively regulating the decision-making process in which that data is employed.

It is also important not to overstate Article 22. The GDPR does not prohibit all automated decision-making. Its exceptions are legally significant, and the provision concerns decisions based solely on automated processing that meet the relevant effects threshold. A decision involving meaningful human participation may fall outside the provision, depending on the actual circumstances.

7.4 Transparency and access to information

The GDPR contains detailed transparency obligations. Articles 13 and 14 require information to be provided to data subjects in specified circumstances. Article 15 provides a right of access

ISSN: 2582-6433

to personal data and related information. Where relevant, these provisions include information concerning the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing.

The DPDP Act provides rights concerning information about personal data, correction, erasure, grievance redressal and nomination, subject to its statutory provisions and limitations. However, it does not establish a directly equivalent set of automated-decision transparency rights in the same form as the GDPR provisions.

For public administration, this distinction matters. Access to personal data is not necessarily the same as access to the reasons for an administrative decision. A citizen may know which information was processed but remain unable to understand why the government rejected an application or assigned a particular risk classification.

India should therefore consider a separate obligation requiring public authorities to provide meaningful reasons where AI materially influences an adverse administrative decision. Such an obligation should be framed in a manner that protects legitimate security and confidentiality interests without permitting those interests to become a blanket justification for opacity.

7.5 Accountability and impact assessments

The GDPR adopts an accountability-based approach. Article 24 requires controllers to implement appropriate measures to ensure and demonstrate compliance. Article 25 addresses data protection by design and by default. Article 32 concerns security of processing, while Article 35 requires a Data Protection Impact Assessment in specified circumstances involving likely high risks to the rights and freedoms of natural persons.

The DPDP Act also imposes obligations on Data Fiduciaries and provides for additional obligations applicable to Significant Data Fiduciaries. The statutory framework therefore recognises organisational responsibility and risk-related compliance.

Nevertheless, the GDPR's DPIA architecture is more explicitly developed as a structured assessment of high-risk processing. It requires consideration of the nature, scope, context and purposes of processing, the risks to individuals and the measures intended to address those risks.

For AI in public administration, the GDPR model offers a useful lesson: risk assessment should occur before deployment and should be reviewed when the nature or consequences of processing change. India could extend this approach through a dedicated algorithmic or fundamental rights impact assessment for public-sector systems that materially affect

ISSN: 2582-6433

individuals.

7.6 Supervisory institutions and enforcement

The GDPR requires independent supervisory authorities and provides a detailed institutional framework for monitoring and enforcing compliance. It also provides for cooperation among supervisory authorities and establishes the European Data Protection Board.

The DPDP Act provides for the Data Protection Board of India and establishes a statutory framework for dealing with contraventions. The institutional models differ in structure, powers and the broader regulatory environment in which they operate.

A central issue for India is not simply whether an enforcement institution exists, but whether it has adequate independence, technical capacity, resources and practical authority to scrutinise complex public-sector processing. Effective oversight requires the ability to obtain relevant information, examine compliance and ensure that statutory obligations are not weakened by the institutional position of the public authority involved.

7.7 Government exemptions and public interest processing

Both frameworks recognise that certain public-interest functions may require data processing without ordinary consent arrangements. Neither framework should be understood as making government processing unrestricted.

The GDPR permits processing on legal bases including public tasks and official authority, subject to the Regulation's requirements. Article 23 allows certain restrictions by Union or Member State law where the prescribed conditions are satisfied. Such restrictions must meet requirements of necessity and proportionality in a democratic society.

The DPDP Act contains provisions concerning specified legitimate uses and exemptions. Their application must be assessed in accordance with the statutory text, commencement position and relevant constitutional requirements.

For India, the key concern is ensuring that broad public-interest objectives do not displace meaningful safeguards. Government processing may be necessary for welfare, public health, security and administration, but the existence of a public purpose should not automatically establish that every form of data aggregation, profiling or automated decision-making is lawful.

ISSN: 2582-6433

7.8 Comparative table

Area	India: DPDP Act, 2023	European Union: GDPR
Primary regulatory focus	Processing of digital personal data	Processing of personal data within the GDPR's scope
Core principles	Statutory framework covering notice, consent, specified uses, fiduciary duties and individual rights	Express principles under Article 5, including fairness, transparency, purpose limitation and accountability
Automated decision-making	No directly equivalent general provision to Article 22	Article 22 addresses certain solely automated decisions with legal or similarly significant effects
Transparency	Notice and individual rights under the Act	Detailed information and access rights under Articles 13–15
Impact assessments	Obligations for specified categories and circumstances under the Act and Rules	Data Protection Impact Assessments under Article 35 for likely high-risk processing
Special categories of data	No directly equivalent general category structure to GDPR Article 9	Specific restrictions on special categories under Article 9
Supervisory framework	Data Protection Board of India	Independent national supervisory authorities and EU cooperation mechanisms
Government processing	Specified legitimate uses and statutory exemptions	Public-task and official-authority legal bases, with restrictions subject to GDPR requirements
AI-specific regulation	AI governance primarily addressed through policy guidance and existing laws	GDPR supplemented by the AI Act's risk-based obligations
Current implementation position	Staggered commencement under the 2025 notifications	GDPR has applied since 25 May 2018

The comparison demonstrates that the two systems are not simply different versions of the same regulatory model. The GDPR offers more detailed provisions concerning certain

ISSN: 2582-6433

automated decisions, transparency and data protection impact assessments. India's framework has its own statutory design and constitutional foundations, but it does not yet provide an equivalent comprehensive set of safeguards directed specifically at algorithmic public decision-making.

7.9 The AI Act as a complementary European instrument

The EU AI Act must be distinguished from the GDPR. The GDPR regulates personal data processing; the AI Act establishes harmonised rules concerning specified AI practices, high-risk systems and operator obligations.

A particularly relevant provision for public administration is Article 27, which requires specified deployers of high-risk AI systems, including bodies governed by public law and certain private entities providing public services, to undertake a fundamental rights impact assessment before deployment, subject to the provision's scope and exceptions.

The assessment considers the intended processes, the period and frequency of use, the categories of persons likely to be affected and the specific risks of harm. The provision demonstrates a regulatory approach that looks beyond the processing of personal data and directly considers the impact of AI deployment on fundamental rights.

This is especially relevant to India. A welfare eligibility system, public employment screening tool or law enforcement risk assessment system may raise concerns that cannot be adequately addressed through data protection compliance alone. A separate assessment of the effects on equality, liberty, access to public services and procedural rights may therefore be necessary.

8. Judicial and Comparative Lessons for Algorithmic Accountability

8.1 *State v. Loomis*: caution in algorithmic sentencing

The Wisconsin Supreme Court's decision in *State v. Loomis* concerned the use of the COMPAS risk assessment tool in criminal sentencing. The court permitted the use of the assessment subject to warnings and limitations, recognising that the tool should not be treated as an independent or determinative basis for sentencing.

The case illustrates the importance of maintaining judicial responsibility where algorithmic assessments are used in criminal justice. A statistical risk score cannot replace the court's obligation to consider the legally relevant circumstances of the individual case.

For India, the broader lesson is that AI-generated recommendations should not become substitutes for legally required judicial or administrative reasoning. Where an algorithm influences a decision, the responsible authority must retain the ability and obligation to examine

ISSN: 2582-6433

the underlying information and exercise independent judgment.

8.2 The SyRI judgment: privacy and proportionality in public administration

In *NJCM and Others v. The Netherlands*, concerning the System Risk Indication (SyRI), the District Court of The Hague examined a government system used to identify possible fraud through the combination and analysis of personal data. The court found that the legislative framework did not provide a sufficiently fair balance between the public interest in fraud prevention and the interference with private life under Article 8 of the European Convention on Human Rights.

The case is important because it demonstrates that the public objective of preventing fraud does not automatically justify extensive data processing and opaque risk profiling. The design of the system, the safeguards available and the ability of affected persons to understand the process are central to the legality assessment.

The judgment offers a comparative lesson for Indian welfare administration. Fraud prevention is a legitimate public objective, but the use of algorithmic profiling must remain subject to necessity, proportionality, transparency and adequate safeguards.

8.3 *R (Bridges) v Chief Constable of South Wales Police*: facial recognition and public law

In *R (Bridges) v Chief Constable of South Wales Police*, the UK Court of Appeal considered the use of automated facial recognition by the police. The court identified legal deficiencies in the framework governing the deployment of the technology, including concerns relating to the discretion over where the technology could be used and who could be placed on watchlists. The case also considered data protection and the public sector equality duty.

The decision demonstrates that public authorities must establish sufficiently clear legal and operational limits when deploying intrusive technologies. The mere availability of facial recognition does not establish that its use is lawful in every context.

For India, this reinforces the importance of legal authorisation, defined deployment conditions, equality assessments and judicially reviewable safeguards for AI-enabled surveillance.

9. The Regulatory Gap: Why Data Protection Alone Is Insufficient

The preceding analysis reveals a conceptual problem in treating data protection as a complete solution to AI governance. Data protection law regulates the collection, use, storage and disclosure of personal information. AI governance must additionally address the consequences of the decisions and classifications produced through algorithmic systems.

ISSN: 2582-6433

Four distinct but interconnected gaps can be identified.

9.1 The decision-making gap

Data protection compliance does not necessarily establish that an administrative decision is rational, fair or lawful. An algorithm may use personal data lawfully but still produce an arbitrary or discriminatory outcome. The decision-making process therefore requires independent legal scrutiny.

9.2 The explainability gap

Rights of access to personal data do not always provide an adequate explanation of the reasoning behind an algorithmically influenced decision. Public authorities should be required to communicate the material reasons for adverse decisions in a form that affected individuals can understand and challenge.

9.3 The accountability gap

AI systems may involve multiple actors, including government departments, technology providers, data processors and external consultants. Where responsibility is divided contractually or technically, individuals may face difficulty identifying the institution answerable for an adverse outcome.

Public authorities should remain responsible for the legality of decisions taken in the exercise of public power, even where technical functions are outsourced. Procurement arrangements should therefore preserve government access to relevant records, audit information and technical documentation.

9.4 The remedy gap

An effective legal framework must provide more than general principles. It must allow individuals to obtain correction, reconsideration and appropriate remedies. A person who is wrongly denied a public benefit because of an algorithmic error should not be required to navigate an inaccessible technical process before receiving a fair administrative review.

The combined effect of these gaps suggests that India requires a more explicit framework for algorithmic accountability, particularly in high-impact public-sector applications.

ISSN: 2582-6433

10. Towards a Rights-Based Framework for AI in Indian Public Administration

A suitable Indian framework should build upon existing constitutional and statutory protections rather than treating AI governance as an entirely separate regulatory field. It should also avoid the assumption that the European model can be transplanted without adjustment. India's administrative structure, socioeconomic conditions, digital infrastructure and institutional capacities require a context-sensitive approach.

The following reforms are proposed.

10.1 Statutory recognition of high-impact algorithmic decision-making

India should consider introducing specific statutory obligations for AI systems that materially influence decisions concerning fundamental rights, public benefits, law enforcement, employment in public institutions and access to essential services.

The framework should distinguish between low-impact administrative automation and high-impact systems capable of affecting legal status, liberty, livelihood or access to public entitlements.

A risk-based approach would allow proportionate regulation without subjecting every administrative software application to the same level of scrutiny.

10.2 Mandatory algorithmic and fundamental rights impact assessments

Public authorities should be required to undertake an impact assessment before deploying high-impact AI systems. Such assessments should examine:

The purpose and legal basis of the proposed deployment.

- The categories of individuals likely to be affected.
- The nature and quality of the data used.
- Potential discriminatory effects.
- The consequences of inaccurate outputs.
- The availability of human review.
- The accessibility of complaint and redress mechanisms.
- The arrangements for independent auditing.

The assessment should be periodically reviewed, particularly when the system's purpose, dataset or operational environment changes. The GDPR's Article 35 DPIA model and the AI Act's Article 27 fundamental rights impact assessment provide useful comparative references,

ISSN: 2582-6433

although an Indian framework should reflect the requirements of Articles 14 and 21.

10.3 Meaningful human oversight

Human oversight should be mandatory where AI materially influences decisions carrying serious consequences for individuals. However, the requirement should not be satisfied by merely placing an official between the algorithm and the final administrative order.

The reviewing official should have adequate training, access to relevant information and authority to reject the system's recommendation. The official should also record the reasons for accepting or departing from the algorithmic output where the decision has significant consequences.

10.4 A right to intelligible reasons and effective review

Individuals affected by high-impact AI-assisted administrative decisions should receive intelligible information concerning the material grounds of the decision. This should include, where appropriate, the fact that an AI system materially influenced the outcome, the principal factors relevant to the decision and the process for requesting human reconsideration.

The proposed safeguard need not require public disclosure of every line of source code. Legitimate interests involving security, privacy and intellectual property may require carefully tailored protections. Such interests should not, however, prevent courts and authorised regulators from accessing information necessary to examine the legality of the system.

10.5 Independent auditing and institutional capacity

High-impact public-sector AI systems should be subject to independent audits at appropriate intervals. Audits should examine accuracy, data quality, security, discriminatory effects, performance across affected groups and compliance with applicable legal requirements.

India should also strengthen the technical capacity of existing regulators and oversight institutions. Effective regulation requires personnel who understand both the relevant legal standards and the technical characteristics of AI systems.

10.6 Transparency in public procurement

Public procurement is an important stage at which accountability safeguards can be incorporated. Contracts with AI developers and service providers should address access to technical documentation, audit rights, data protection responsibilities, security obligations, record retention and cooperation with judicial or regulatory scrutiny.

ISSN: 2582-6433

A government authority should not be able to avoid its public-law obligations by relying on contractual confidentiality provisions or the proprietary nature of a privately developed algorithm.

10.7 Public participation and accessible remedies

Communities likely to be affected by high-impact AI deployments should have an opportunity to participate in consultation processes. Public authorities should publish appropriate information about the purpose, risks and safeguards of significant systems.

Individuals should also have accessible complaint mechanisms, human reconsideration procedures and routes to existing statutory and constitutional remedies. The objective should be to ensure that the burden of identifying and correcting systemic errors does not fall entirely upon vulnerable individuals.

11. Discussion: Balancing Innovation, Administrative Efficiency and Constitutional Legitimacy

The regulation of AI in public administration involves a continuing tension between innovation and the protection of individual rights. Excessively rigid rules may discourage beneficial technological applications, particularly where AI can improve access to healthcare, education, welfare and other public services. On the other hand, a regulatory approach that relies primarily on voluntary commitments may provide insufficient protection where the consequences of error are serious.

The appropriate response is neither unrestricted technological adoption nor a general prohibition on AI-assisted administration. It is a proportionate framework that distinguishes between applications according to their purpose, potential impact and the rights affected.

The European experience demonstrates the value of combining data protection with AI-specific obligations. The GDPR addresses the processing of personal data, while the AI Act introduces additional requirements for specified high-risk systems. This layered model is instructive for India because it recognises that the legality of data processing and the legitimacy of an AI application are related but distinct questions.

India's constitutional framework can provide the normative foundation for such an approach. Article 14 requires public authorities to avoid arbitrary and discriminatory action; Article 21 protects liberty, dignity and privacy; and administrative law principles require fair procedures and legally defensible decisions. These protections should inform the entire lifecycle of public-

ISSN: 2582-6433

sector AI, from procurement and design to deployment, monitoring and review.

At the same time, regulatory design must account for institutional capacity. A sophisticated statutory framework will have limited practical value if public authorities lack technical expertise, regulators cannot inspect systems or individuals cannot access effective remedies. The implementation of AI governance therefore requires investment in institutional knowledge, public-sector training and independent oversight.

Ultimately, the question is not whether AI should participate in government decision-making. The more important question is under what legal conditions it may do so. A democratic state may use technology to improve administration, but it cannot delegate away its responsibility to act fairly, rationally and consistently with fundamental rights.

12. Conclusion

The integration of artificial intelligence into public administration presents an important opportunity to improve the delivery of public services and the efficiency of government institutions. However, the increasing influence of algorithmic systems over decisions affecting individual rights and entitlements requires a corresponding development of legal safeguards. The risks associated with algorithmic bias, opacity, intrusive data processing and fragmented responsibility demonstrate that technological efficiency cannot serve as the sole measure of administrative legitimacy.

India possesses important constitutional and statutory foundations for addressing these concerns. Articles 14 and 21, the privacy jurisprudence developed in *Puttaswamy*, the DPDP Act, 2023 and the India AI Governance Guidelines, 2025 collectively provide a basis for responsible AI deployment. Nevertheless, these instruments do not yet constitute a comprehensive and enforceable framework for algorithmic accountability in public administration. In particular, data protection legislation cannot independently resolve questions concerning discriminatory administrative outcomes, reasoned decision-making, meaningful human review and remedies against algorithmically influenced public decisions.

The comparison with the GDPR reveals important areas from which India may draw regulatory lessons. The GDPR's provisions concerning automated individual decision-making, transparency, accountability and data protection impact assessments provide a more developed statutory response to certain risks associated with personal data processing. The EU AI Act further demonstrates the value of complementing data protection with risk-based and fundamental rights-oriented AI obligations. These mechanisms should be considered as comparative models rather than provisions to be imported without adaptation.

ISSN: 2582-6433

This paper has argued that India should develop a rights-based framework for high-impact AI in public administration, grounded in constitutional principles and supported by enforceable procedural safeguards. Such a framework should require appropriate impact assessments, meaningful human oversight, intelligible reasons, independent auditing, transparent procurement and accessible redress mechanisms. It should also preserve the responsibility of public authorities for decisions taken with the assistance of privately developed technological systems.

The future of AI governance in India should not be measured merely by the speed at which public institutions adopt new technologies. Its success must also be assessed by whether those technologies strengthen, rather than weaken, the relationship between the state and the citizen. AI can make public administration more capable, but only constitutional accountability can make its exercise of power legitimate.

IJLRA