IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Balancing AI Efficiency And Privacy Rights In Public Sector Governance

Varsha G Nair, Research scholar, HITS, CHENNAI, INDIA

ABSTRACT

The increasing adoption of artificial intelligence (AI) in public administration offers significant opportunities to enhance efficiency, accuracy, and service delivery. AI-driven systems can improve decision-making, automate routine administrative tasks, and enable data-informed policy development. However, the extensive use of personal and sensitive data in these systems raises critical concerns regarding privacy, data protection, and individual rights. This paper examines the challenge of harmonizing AI efficacy with privacy rights in the public sector. It analyses how public administrations can leverage AI's benefits while complying with legal, ethical, and constitutional privacy obligations. The study explores key risks such as data misuse, algorithmic bias, lack of transparency, and accountability gaps, alongside existing and emerging regulatory frameworks for data protection and AI governance. It further highlights best practices, including privacy-by-design, data minimization, explainable AI, and robust oversight mechanisms, as tools for balancing innovation with rights protection. The paper concludes that sustainable and trustworthy AI deployment in public administration requires an integrated approach that aligns technological advancement with strong legal safeguards, ethical standards, and public trust.

INTRODUCTION

AI is such a transformative and promising element of data-based governance, trade, and communication that AI-powered facial recognition, predictive analytics, and automated decision-making depend significantly on the collection and processing of huge amounts of personal data from people.[1] These take us into the unexplored tracks for which we are unprepared; such technology usually comes with no real and clear legal safeguards for the protection of privacy.[2] Mass surveillance risks, data breaches, and loss of individual autonomy render technical advancements like facial recognition, predictive analytics, and algorithmic profiling significant challenges to traditional privacy rights.[3]

The Growing Role of AI in Public Administration

AI has become an increasingly integral component of public sector operations. In areas such as healthcare, taxation, social welfare, law enforcement, and urban planning, AI systems are being used to process large datasets, predict trends, and automate routine administrative tasks. For instance, AI can assist in identifying welfare fraud, optimizing public transport routes, managing public health crises, and improving citizen engagement through digital platforms.

The appeal of AI lies in its ability to enhance speed, accuracy, and consistency in administrative processes. By automating repetitive tasks, AI allows public servants to focus on strategic planning and human-centered

[1] KATE CRAWFORD, ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE 1-21 (Yale University Press 2021).

[2] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 556 (2006).

[3] Paul Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1865-1879 (2011).

services. In resource-constrained environments, AI can also reduce operational costs and improve outcomes, making governance more effective and responsive to public needs.

Understanding AI and Privacy Rights- Legal and Ethical Challenges in AI

The right to privacy exists to offer inalienable protection against any unauthorized interference-individual or collective-from public or private sources. Today, digital privacy incorporates a broad variety of circumstances linked to physical space and communication, including safeguarding of information and self-determination. Courts across the global legal systems have regularly asserted that the central role of privacy comes from its critical ability to uphold human dignity, personal autonomy, and individual liberty.[4]
In the landmark judgment of *K.S. Puttaswamy v. Union of India (2017)*, the right to privacy was declared to be a fundamental right protected under Article 21 of the Constitution.[5] Similarly, the international frameworks, ECHR and UDHR, suggest privacy is among the core human rights. However, AI-based technologies constantly pose challenges to these protections: the automation of surveillance, profiling of individuals, and behavior predictions, often without consent.[6]

Privacy Risks and Ethical Concerns

Despite its advantages, AI in public administration raises serious privacy concerns. AI systems often rely on vast amounts of personal data, including sensitive information such as health records, financial details, biometric data, and location tracking. The collection, storage, and processing of such data increase the risk of data breaches, misuse, and unauthorized surveillance.

Moreover, AI systems can unintentionally reinforce discrimination or bias if they are trained on flawed or unrepresentative data. Automated decision-making without sufficient human oversight may lead to unjust outcomes, particularly for vulnerable populations. When citizens do not understand how decisions affecting them are made, transparency and accountability are weakened.

Privacy rights are fundamental human rights. If individuals feel constantly monitored or fear that their personal data is being exploited, public confidence in government institutions may erode. Therefore, public administrations must ensure that technological efficiency does not come at the expense of civil liberties.

Gaps in Legal and Regulatory Frameworks

Though several privacy laws have sought to regulate data protection, like the GDPR, CCPA, and DPDPA (2023), they regulate without an AI-specific reference.

1. General Data Protection Regulation (GDPR):
   a) Strengths: Data minimization, purpose limitation, and user consent are necessary for AI-based data processing.[7]
   b) Weaknesses: Lack of explicit references to AI biases, algorithmic accountability, and explainability.[8]
2. California Consumer Privacy Act (CCPA):
   a) Strengths: It allows users the ability to opt out of collecting data and seek the erasure of personal information.[9]
   b) Weaknesses: It doesn't cover AI-based profiling, automated decision-making, and inferences on data.
3. India’s Digital Personal Data Protection Act (DPDPA), 2023:

[4] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934-1965 (2013).

[5] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

[6] U.N. Special Rapporteur on the Right to Privacy, *Report on Artificial Intelligence and Privacy*, U.N. Doc. A/HRC/43/52 (2020).

[7] Regulation (EU) 2016/679, of the European Parliament and of the Council, of 27 April 2016, *on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC* (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[8] Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”*, 38 AI Magazine 50, 50-57 (2017).

[9] California Consumer Privacy Act, § 100-199 (1798).

a) Strengths: It introduces data localization requirements, consent-based processing, and obligations for data fiduciaries.[10]

b) Weaknesses: It does not include stringent governance provisions regarding AI in general and specifically regarding AI bias, fairness of algorithms, and regulatory oversight.

Need for a Comprehensive AI Privacy Framework

Considering the eminent transformative effects that AI has had in the field of privacy, the legal mechanisms in place should be amended in terms of norms that specifically regulate AI. Key policy recommendations are as follows:

- Transparency & Explainability: AI systems ought to give clear justifications for all of their decisions impacting individuals.
- Bias Audits & Ethical AI Standards: Regular audits of AI decision-making on issues of bias and fairness are to be made compulsory.
- Stronger Regulatory Oversight: Creating an AI Ethics Board to monitor compliance with established norms of AI privacy.
- Enhanced User Control: Expanding rights of users, including explanation, redress, and algorithmic contestation for people assisted by AI.

All these ethical challenges call specifically for transparent, accountable, and fair systems for regulating AI.[11]

Ethical AI and Responsible Governance

Beyond legal compliance, ethical considerations play a crucial role in harmonizing AI and privacy. Ethical AI in public administration requires fairness, explainability, and human oversight. Citizens should be informed when AI systems are used in decision-making processes that affect them, and they should have access to explanations and appeal mechanisms.

Responsible governance also involves limiting data collection to what is strictly necessary and ensuring robust cybersecurity measures. Privacy-by-design approaches—where privacy protection is built into AI systems from the outset—can significantly reduce risks. Training public officials to understand AI technologies and their ethical implications is equally important.

Legal and Policy Recommendations for AI and Privacy Protection

In transforming several domains of human decision-making, AI raises significant questions regarding the protection of privacy and requires a strong regulatory regime. The challenges of data protection recognized in legal frameworks such as the GDPR and India's DPDPA, 2023 have, within some parameters, been articulated; however, these efforts have a poor regard for AI-specific guarantees. Accordingly, a regulatory approach should support AI-aided decisions in their transparency, accountability, and fairness orientation while incorporating global best practices.

❖ Strengthening Transparency and Explainability

AI-embedded decision-making systems are characterized by poor transparency, raising multiple apprehensions around fairness, accountability, and due process. Thus, legal frameworks should mandate:

- Algorithmic Transparency Duties: AI systems must provide suitable explanations for the choices made that affect individuals. Article 22 of the GDPR grants individuals a right to receive "meaningful information" relating to the automated decision making that has any effect on them. However, this is too limited, since the obligation does not provide for full disclosure of AI models.[12] Additional transparency initiatives should be introduced.
- Algorithmic Impact Assessments (AIA): Based on the Data Protection Impact Assessment (DPIA) under article 35 of GDPR, the AIA is intended to evaluate, beforehand, possible risks of bias, discrimination,

[10] Digital Personal Data Protection Act, 2023, §§ 8, 12, 16, No. 22, Acts of Parliament, 2023 (India).

[11] European Commission Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (Apr. 8, 2019, 10:20 PM), https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf.

[12] Council Regulation (EU) 2016/679, *supra* note 18, art. 22.

and privacy violations related to AI deployment.[13] The EU's proposed AI Act takes a similar path and prescribes risk categorization of AI applications by their potential harm.[14]

- Explainability Standards: AI models must be able to give explicit reasons for their decisions, especially in high-risk cases like credit scoring and criminal justice. The OECD AI Principles (2019) point out that AI systems should be "transparent and explainable" to ensure accountability. [15]

❖ Addressing Bias and Discrimination

AI systems tend to represent biases contained within their training data, and this could lead to unfair treatment targeted toward marginalized groups. Legal frameworks should address this through:

- Algorithmic audits specify that there should be regular assessments of AI models to see whether they may be producing discriminatory outcomes. The 2008 BIPA has set a precedent by enforcing accountability on AI-based face recognition technologies.[16] A similar model can be adopted in broader AI applications.
- Right to Contest AI Decisions: Rights established in the GDPR provide individuals substantial options to contest discriminatory behavior in decisions affecting them by automated means, but implementation is weak. Providing this stipulation strength through the imposition of mandatory human review of decisions made by AI, notably in hiring, police, and financial services, would improve fairness.[17]
- Prohibition of Discriminatory AI Practices: There should be express provisions of laws prohibiting any AI model that results in systematic discrimination. Such is the case for the USA's Equal Credit Opportunity Act (ECOA), which prohibits discrimination in credit assessments.[18] AI-driven credit scoring systems must be reviewed for compliance with such non-discrimination criteria.

❖ Measure for Strengthening Privacy Protections

AI can process humongous amounts of personal data; hence, privacy laws must mandate stricter measures such as:

- Enhanced Consent Mechanisms: Under the current GDPR (Articles 6 and 7), consent must be informed and explicit. Indeed, AI model inference may involve sensitive characteristics that appear without explicit user input. Section 6 of DPDPA, 2023, should include a clear prohibition on AI profiling without explicit consent.[19]
- Right to Opt-Out of AI Profiling: The user should have a right to opt-out of profiling by AI systems, in line with the opt-out provisions of the California Consumer Privacy Act (2018);[20] this will enhance the control of people over the use of their data.
- Data Minimization Requirements: Under Article 5(1)(c) of the GDPR,[21] the AI systems should collect only the data that is necessary concerning their purpose. It should be ensured with stringent compliance measures attached to enhanced penalties.

❖ Regulatory Oversight and Governance

Under the complex governance of AI, a specialized independent regulatory authority is needed for oversight and enforcement. Recommended measures would include:

- Formation of an AI Regulatory Authority: A regulatory authority dedicated to AI is needed to supervise compliance with standards of privacy and fairness. Similar to the European Data Protection Supervisor (EDPS), which looks into the compliance of laws in the EU on data protection.[22] A similar authority specialized in AI should be formed in India under the DPDPA.

[13] Council Regulation (EU) 2016/679, *supra* note 18, art. 35.

[14] European Commission, *Regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* (Mar. 15, 2025, 10:45 AM), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206#:~:text=This%20proposal%20imposes%20some%20restrictions,rights%20('responsible%20innovation'.

[15] OECD, *AI principles* (Mar. 16, 2025, 11:27 AM),https://www.oecd.org/en/topics/sub-issues/ai-principles.html.

[16] 740 ILCS 14/1 (Illinois); Illinois General Assembly, Illinois Compiled Statutes, (Mar. 20, 2025, 02:23 PM) https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004.

[17] Council Regulation (EU) 2016/679, *supra* note 18, art. 22.

[18] 15 U. S. Code. § 1691 (2012).

[19] Digital Personal Data Protection Act, 2023, *supra* note 16, § 6.

[20] California Consumer Privacy Act (2018).

[21] Council Regulation (EU) 2016/679, *supra* note 18, art. 5(1)(c).

[22] European Data Protection Supervisor, *Our role as a supervisor,* Our role as a supervisor | European Data Protection Supervisor (Mar. 26, 2025, 08:45 AM), https://www.edps.europa.eu/data-protection/our-role-supervisor_en.

- Mandatory Registration for High-Risk AI Systems:
- While a proposed AI Act in the European Union introduces the classification of risk requiring stringent regulatory scrutiny of high-risk AI applications,[23] something similar should be approved globally with legislation obliging AI developers to register and disclose their models.
- Stronger Enforcement Mechanisms: AI-powered platforms that violate users' privacy should face greater penalties. Non-compliance with Article 83 of the GDPR can attract fines maximum of €20 million or 4% of global sales.[24] India's DPDPA (Section 33) imposes financial penalties; however, they should be raised for AI-related violations.

Conclusion

AI has the potential to revolutionize public administration by making government services more efficient, responsive, and data-driven. However, these benefits must be carefully balanced against the need to protect privacy rights and uphold ethical standards. Harmonizing AI efficacy and privacy rights requires robust legal frameworks, ethical governance, transparency, and active citizen engagement.

By adopting responsible AI practices, public administrations can ensure that technological progress strengthens rather than undermines public trust. The challenge is not choosing between efficiency and privacy, but designing systems that respect both. When properly balanced, AI can become a powerful tool for good governance in a democratic society.

[23] European Commission, *supra* note 34.
[24] Council Regulation (EU) 2016/679, *supra* note 18, art. 83.