INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 6 [2025] | Page 115 - 122

A CONSTITUTIONAL FRAMEWORK FOR REGULATING AI-DRIVEN GOVERNMENT SURVEILLANCE: BALANCING PRIVACY, SECURITY, AND TECHNOLOGICAL INNOVATION (2025)

- Sruti Jose Alex [1]

ABSTRACT

The rapid adoption of AI-driven surveillance technologies such as biometric monitoring, facial recognition, and predictive analytics raises constitutional concerns[2], which are examined in this study. The primary problem discussed is the absence of a precise constitutional framework that reconciles the essential right to privacy with the necessity of national security. The study's objectives are to evaluate current legal norms, analyse proportionality requirements, and propose constitutional safeguards for responsible AI use. According to the theory, AI-enabled surveillance can be constitutionally compliant with clear, necessity-based restrictions, but if left unchecked, it could result in disproportionate and opaque state power.

A review of the literature reveals a lot of research on digital privacy but not much on incorporating AI into constitutional doctrines. This indicates a lack of research on structured constitutional principles designed with algorithmic surveillance in mind. Doctrinal analysis, comparative constitutional analysis, and assessment of new AI governance models are all part of the methodology. Offering a rights-protective model appropriate for democracies is what makes it significant. According to preliminary research, the current body of privacy law is inadequate for the complexity of AI. A multi-layered constitutional framework based on accountability, proportionality, and transparency is suggested in the conclusion.

[1] Christ Academy Institute of Law.

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

Keywords: digital governance, proportionality test, AI surveillance, constitutional law, privacy rights, and facial recognition.

INTRODUCTION

Artificial intelligence (AI) has revolutionised state surveillance capabilities through facial recognition systems, biometric identification networks, predictive policing tools, and large-scale data monitoring technologies. Although these systems improve efficiency and national security, they also compromise long-standing constitutional protections. The landmark decision in Justice K.S. Puttaswamy v. Union of India (2017) in India elevated privacy to the status of a fundamental right while highlighting autonomy, dignity, and informational self-determination as essential constitutional values. However, the ruling did not fully account for the extraordinary expansion of AI-enabled surveillance currently employed in public administration, governance, and policing. Real-time biometric surveillance is categorised as "high-risk" in the European Union's AI Act (2024), and the UN Human Rights Council (2021) warns that unchecked AI surveillance can endanger civil liberties and democratic accountability. All democratic governments worldwide share these worries. These developments highlight the urgent need for India and other constitutional democracies to embrace a constitutional approach to AI surveillance that is rights-centered.

The complexity of AI-driven systems, particularly their predictive nature, opacity, and potential for automated decision-making without human oversight, often falls outside the purview of current constitutional jurisprudence, which emerged during a period of analogue forms of surveillance and physical searches.

The challenge of promoting technological innovation while avoiding abuse, prejudice, and the development of a surveillance state is being faced by courts and legislatures worldwide. Therefore, a structured constitutional framework that guarantees the responsible and rights-balanced use of AI in surveillance practices is desperately needed[3]. In order to ensure that state power is both effective and accountable in the digital age, this study looks at how constitutional principles—such as proportionality, due process, equality, and the right to privacy—can be modified and reinforced to meet the realities of emerging AI technologies.

[3] Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Open University Press, 2001.

RESEARCH PROBLEM

The lack of a comprehensive constitutional framework governing India's use of AI-driven surveillance systems is the main research issue. The Information Technology Act of 2000, policing statutes, and the Digital Personal Data Protection Act of 2023 are examples of current legal frameworks that are insufficient for technologies that can perform biometric profiling, automated monitoring, and real-time data analysis. Among the new problems that AI systems bring are behavioural prediction, algorithmic discrimination, mass data extraction, lack of transparency, and limited channels for redress. Traditional safeguards, such as warrants, reasonable restrictions, and judicial oversight, were developed for human-directed surveillance rather than automated systems that could track individuals continuously and extensively. As a result, there is a constitutional gap, and AI-enabled surveillance endangers fundamental rights like equality, due process, and privacy in the absence of strict regulation.

OBJECTIVE

This study's main goal is to critically investigate how constitutional principles can be used to control AI-driven government surveillance in a way that strikes a balance between people's right to privacy and the justifiable needs of public order and national security[4]. This study aims to determine whether current constitutional protections—specifically, the right to privacy, proportionality standards, due process protections, and equality guarantees—are sufficient to mitigate the risks associated with cutting-edge surveillance technologies like biometric monitoring, facial recognition, predictive analytics, and extensive data mining.In order to create a logical and technologically advanced regulatory framework, the study also seeks to pinpoint the weaknesses and inconsistencies in the current judicial and legislative approaches, both in India and in similar constitutional democracies. Another goal is to evaluate how the State's use of AI systems can be constitutionally integrated with accountability, transparency, and human oversight. The study's ultimate goal is to provide practical constitutional guidelines that guarantee AI-enabled surveillance stays legitimate, essential, reasonable, and consistent with democratic principles[5].

[4] *Riley v. California*, 573 U.S. 373 (2014)
[5] European Union. *EU Artificial Intelligence Act* (2021–2024 versions).

HYPOTHESIS

The study's premise is that AI-driven government surveillance poses a serious risk of disproportionate invasion of personal privacy and may allow arbitrary or discriminatory State action in the absence of clear constitutional protections. However, a well-structured constitutional framework founded on the values of legality, necessity, proportionality, transparency, and accountability can effectively lower these risks. As long as lawmakers and courts consider technological realities like algorithmic opacity, data-driven profiling, and automated decision making in their rights-based analyses, it is also anticipated that existing constitutional doctrines which were first developed for traditional forms of surveillance can be modified to govern new AI technologies. Thus, the hypothesis is based on the notion that a regulatory model informed by the constitution can both protect fundamental rights and allow the State to use AI for legitimate security purposes without endangering democratic values.

LITERATURE REVIEW

While existing research offers insightful viewpoints, it clearly falls short in addressing constitutional issues unique to AI. The Supreme Court's judgment in Puttaswamy established privacy as a fundamental right and introduced the proportionality test as the constitutional standard for evaluating intrusions by the State. According to academics like Dwork and Paternoster (Yale Law Journal, 2020), conventional privacy doctrines need to be expanded to take algorithmic opacity and automated decision-making into account Shoshana Zuboff's 2019 book The Age of Surveillance Capitalism demonstrates how AI systems enable unprecedented behavioural monitoring, raising grave concerns about autonomy.

The EU AI Act (2024) mandates strict oversight of high-risk AI systems, such as biometric surveillance, and the US judiciary acknowledged in Carpenter v. United States (2018) that digital surveillance requires more constitutional scrutiny. These developments in international law offer more understanding of regulatory reactions. The Vidhi Centre for Legal Policy (2022) and PRS Legislative Research (2023) conducted research in India that indicates the use of facial recognition technology by law enforcement agencies is not supported by uniform security measures or a legal basis. These sources all highlight problems, but they don't offer a constitutional framework made especially for government monitoring using artificial intelligence.

RESEARCH GAP

The constitutional right to privacy and the effects of digital surveillance have been extensively studied, but there is still a dearth of specialised research on the particular constitutional issues raised by AI-driven government surveillance. Current research frequently examines algorithmic bias, data security, and AI ethics separately rather than incorporating these issues into a thorough constitutional framework specific to state-run surveillance technologies[6].

The majority of the research that is currently available either focusses on general data protection laws or addresses surveillance in conventional contexts without taking into consideration the predictive, autonomous, and opaque nature of AI systems. Additionally, comparative constitutional studies have mostly ignored the ways in which jurisdictions modify accountability procedures, due process requirements, and proportionality tests to match sophisticated AI capabilities. The degree to which current constitutional doctrines can be adjusted to address concerns like algorithmic transparency, automated decision-making, mass data analysis, and possible government abuse of biometric tools is also not well studied[7].

Therefore, in the age of AI-enabled state surveillance, there is a glaring research gap in creating an organised, constitutionally sound regulatory model that balances privacy rights, technological innovation, and national security considerations.

RESEARCH METHODOLOGY

Using a doctrinal and qualitative research methodology, this study examines constitutional principles, court rulings, legislative provisions, and academic commentary that are pertinent to AI-driven government surveillance[8]. The study mostly uses secondary sources, such as constitutional texts, important rulings from the Supreme Court of India and higher courts in comparable jurisdictions like the United States, the European Union, and the United Kingdom, as well as scholarly works, policy papers, and reports from respectable organisations. To investigate how various democracies regulate or attempt to regulate AI-enabled surveillance tools, a comparative constitutional approach is used,

[6] Wachter, S., Mittelstadt, B., & Floridi, L. "Why a Right to Explanation Does Not Exist in the GDPR." *International Data Privacy Law*, 2017

[7] *S. and Marper v. United Kingdom*, ECtHR (2008).

[8] Kuner, Christopher. "Data Protection, Privacy and the Rule of Law." *I-CON Journal*, 2014.

especially with regard to privacy rights, proportionality standards, and oversight mechanisms. A doctrinal analysis of ideas like the right to privacy, the proportionality test, accountability standards, and the legality principle is also included in the study, assessing how well they apply to emerging AI technologies. The methodology also integrates interdisciplinary insights from computer science and technology governance literature to comprehend modern technological realities, which helps to contextualise legal analysis within algorithmic systems' operational mechanisms[9]. The goal of the interpretive, as opposed to empirical, research is to combine legal standards and technological issues into a logical constitutional framework. To guarantee the validity of the results, every source is carefully assessed for authenticity, reliability, and applicability.

RESULTS AND FINDINGS

The results of this study show that, despite their strength in theory, the current constitutional safeguards are insufficient to control the intricacies brought about by AI-driven government monitoring. The doctrinal analysis shows that conventional legal norms, like the proportionality test, due process, and reasonableness requirements, were developed during a period of manual, targeted, and constrained surveillance. AI-enabled systems, on the other hand, have large-scale monitoring, autonomous, and predictive capabilities that enable the State to gather and examine personal data far more thoroughly than courts had previously thought. Judicial precedents, such as the recognition of privacy as a fundamental right and the adoption of proportionality as a constitutional test, offer certain essential protections.

Nevertheless, systemic biases in AI technologies, automated decision-making, and algorithmic transparency are not particularly addressed by these precedents. Additionally, comparative analysis shows that while some jurisdictions—particularly those in developing democracies—still primarily rely on outdated surveillance laws, others—like the European Union—have begun to develop regulatory tools like the AI Act and strict data protection frameworks. One significant finding is that AI-driven surveillance disproportionately affects marginalised communities due to algorithmic biases resulting from skewed datasets. This raises further issues under the principles of equality and non-discrimination. Furthermore, the study finds that the lack of mandatory human oversight, independent audits, and transparency requirements increases the risk of

[9] Buolamwini, Joy & Gebru, Timnit. "Gender Shades." Proceedings of Machine Learning Research (2018).

arbitrary or excessive State power. Overall, the results demonstrate that while AI technologies can enhance national security and administrative efficacy, a constitutionally based regulatory framework is required to ensure accountability, protect privacy, and prevent the abuse of surveillance tools.

ANALYSIS

The analysis shows that the intersection of technological capability and fundamental rights protections is where the constitutional ramifications of AI-driven government surveillance lie. A thorough analysis of judicial reasoning reveals that although courts acknowledge privacy as essential to human liberty and dignity, they have not yet fully addressed the unique characteristics of AI technologies, especially their capacity to produce widespread, automated, and non-consensual monitoring. Although theoretically sufficient, the proportionality test is difficult to apply in practice because AI systems frequently use opaque algorithms, making it difficult for judges or individuals to determine whether rights interferences are actually necessary, minimally restrictive, and proportionate to the stated goal. The analysis also shows that AI surveillance technologies significantly change the balance of power between the government and the people. AI enables widespread monitoring without corresponding oversight mechanisms, in contrast to traditional surveillance, which is resource-intensive and case-specific. Due to this change, constitutional doctrines must be adjusted to include requirements for transparency, algorithmic explainability, and independent oversight. Jurisdictions with stronger data protection and AI governance frameworks are better positioned to protect constitutional rights, while those without such frameworks are more vulnerable to unbridled state power, according to comparisons with global regulatory trends. The analysis emphasises that a constitutionally based regulatory model must incorporate technological realities, guarantee accountability at every stage of AI deployment, and uphold democratic values by prohibiting mass surveillance, discrimination, and misuse.

CONCLUSION

This study comes to the conclusion that although AI-driven government surveillance has enormous potential to improve administrative effectiveness, predictive policing, and national security, it also poses previously unheard-of risks to constitutional rights, especially equality, privacy, and individual liberty. Despite being based on strong principles like proportionality, due process, and the right to privacy, the doctrinal and comparative analysis shows that current constitutional frameworks are

insufficient to handle the large-scale, automated, and opaque nature of AI technologies. The realities of algorithmic surveillance, where data-driven forecasts, machine-learning models, and biometric systems can enable ongoing monitoring without sufficient oversight or accountability, have not yet been fully addressed by courts or legislatures.

The results highlight the critical need for a formal constitutional framework that specifically controls the use of AI in state surveillance operations. To guarantee that AI surveillance stays legal and appropriate[10], such a framework must include strict necessity tests, algorithmic audits, human oversight, mandatory transparency requirements, and data minimisation principles. Furthermore, constitutional protections that maintain equality and stop abuse against vulnerable groups are necessary due to the dangers of discrimination [11]and algorithmic bias. In the end, this study confirms that constitutional rights and technological innovation are not intrinsically incompatible; rather, governments can responsibly use AI while upholding democratic principles and public confidence through fair and rights-oriented regulation.

[10] Zuboff, Shoshana. *The Age of Surveillance Capitalism*. PublicAffairs, 2019.
[11] Council of Europe. *Convention 108+*, 2018.