Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 6; 2025; Page No. 84-86

Received: 05-08-2025
Accepted: 13-10-2025
Published: 11-11-2025

Predictive Policing, AI Surveillance, and Privacy in India: A Legal Analysis under the DPDP Act 2023

[1]Sahil and [2]Dr. Shobhna Jeet

[1]Research Scholar, K. R. Mangalam University, Haryana, India
[2]Supervisor Professor, K. R. Mangalam University, Haryana, India

DOI: https://doi.org/10.5281/zenodo.18221510

Corresponding Author: Sahil

Abstract

The integration of artificial intelligence (AI) into law enforcement, particularly through predictive policing and mass surveillance systems, represents a paradigm shift in crime prevention and public security in India. While promising efficiency, these technologies pose a profound threat to the fundamental right to privacy, enabled by the vast datafication of the Indian populace through projects like Crime and Criminal Tracking Network & Systems (CCTNS) and facial recognition networks. This paper provides a critical legal analysis of this emerging landscape in the context of India's newly enacted Digital Personal Data Protection Act, 2023 (DPDP Act). It argues that while the DPDP Act establishes a foundational framework for data protection, its provisions are critically ill-suited to regulate state-driven surveillance and predictive analytics. The analysis identifies key deficiencies, including: (1) the extensive exemptions granted to the State for "public interest" and "security" purposes, which create a significant carve-out for law enforcement activities; (2) the lack of robust safeguards against automated decision-making and profiling; and (3) the absence of independent, pre-emptive oversight mechanisms. The paper concludes that without significant legislative amendments and judicial interpretation that prioritizes a proportionality-based assessment, the DPDP Act risks becoming a legitimizing facade for a panopticon state, failing to adequately protect citizens from the privacy-invasive potential of AI-driven policing.

Keywords: Predictive Policing, AI Surveillance, Data Protection, DPDP Act 2023, Privacy, Law Enforcement, India, Fundamental Rights, Automated Decision-Making

1. Introduction

The 21st century has witnessed the rapid datafication of society, with law enforcement agencies globally, and in India, increasingly turning to data-driven technologies to predict and prevent crime. "Predictive policing" uses historical crime data, algorithms, and AI to forecast criminal activity and allocate resources, while "AI surveillance" encompasses a suite of tools, including facial recognition technology (FRT), automated number plate recognition, and social media monitoring. Proponents argue these systems enhance efficiency, optimize resource allocation, and move policing from a reactive to a proactive model.

In India, this shift is underpinned by massive state-level data collection initiatives. The Crime and Criminal Tracking Network & Systems (CCTNS), a nationwide network connecting all police stations, creates a centralized database of crime and criminal information. This is increasingly being integrated with Advance Facial Recognition Systems (AFRS) and other surveillance technologies deployed in smart city projects. However, the deployment of these technologies has preceded a robust legal framework to regulate their use, creating a regulatory vacuum where fundamental rights are at stake.

The landmark Supreme Court judgment in Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017) [2] unequivocally recognized the right to privacy as a fundamental right under Article 21 of the Indian Constitution. The Court laid down a proportionality

standard for any state infringement of privacy, requiring the action to be backed by law, necessary for a legitimate aim, and proportionate to the need for such interference. This judgment was the catalyst for the long-delayed Digital Personal Data Protection Act, 2023.

This paper analyses the efficacy of the DPDP Act, 2023, as a legal check on the privacy-invasive practices of predictive policing and AI surveillance. It posits that the Act, in its current form, provides inadequate protections against state surveillance, potentially legitimizing these practices without embedding the necessary procedural and substantive safeguards mandated by the Puttaswamy test.

2. The Landscape of AI-Driven Policing in India

2.1 Predictive Policing: Indian police forces have begun experimenting with predictive policing models. For instance, the "Pol-ICE" initiative in Delhi and the "Project Eye" in Uttar Pradesh aimed to use data analytics to predict crime hotspots. These systems often rely on historical crime data, which is itself a reflection of pre-existing policing biases. The risk of a "feedback loop" is high, where algorithms direct police to already over-policed neighbourhoods, leading to more arrests and reinforcing the algorithm's bias, thereby perpetuating systemic discrimination against marginalized communities.

2.2 Mass Surveillance Infrastructure: India is building one of the world's most extensive surveillance infrastructures

- **Facial Recognition Technology (FRT):** The National Crime Records Bureau (NCRB) has deployed an Automated Facial Recognition System (AFRS) intended to identify criminals, missing persons, and unknown dead bodies by matching against databases like CCTNS. However, its use is expanding to mass surveillance during public events and protests.
- **Centralized Databases:** The integration of CCTNS with other databases (e.g., immigration records, vehicle registration) creates a pervasive surveillance ecosystem. The absence of a data protection law until 2023 meant this integration occurred without clear standards for data processing, purpose limitation, or storage.

These technologies, while powerful, operate with significant opacity, raising concerns about accuracy, algorithmic bias, and the lack of public accountability.

3. The Digital Personal Data Protection Act, 2023: A Flawed Shield?

The DPDP Act, 2023, establishes a comprehensive framework for the processing of digital personal data. However, its application to state surveillance and predictive policing reveals critical shortcomings.

3.1 The Significant Exemptions for the State (Section 17)

The most significant flaw from a surveillance perspective is Section 17 of the Act. It grants the Central Government the power to exempt any instrumentality of the State from the Act's provisions for a range of vague and broad reasons, including:

- The interest of the sovereignty and integrity of India.
- Security of the State.
- Friendly relations with foreign States.
- Maintenance of public order.

This provision effectively creates a massive carve-out for law enforcement and intelligence agencies. The processing of personal data for predictive policing or surveillance can easily be justified under "security of the State" or "maintenance of public order." This blanket exemption undermines the core principles of the Act and fails the Puttaswamy test of being a "law" that is precise and narrowly tailored. It grants the executive unfettered discretion, devoid of the necessary procedural safeguards against abuse.

3.2 Weakened Principles of Data Processing

Even if the state exemption is not invoked, the core principles of the Act are diluted when applied to law enforcement.

- **Notice and Consent:** The concept of "deemed consent" under Section 7 includes instances where an individual "voluntarily" provides personal data. In public spaces under pervasive surveillance, the notion of voluntary provision is fictional. Furthermore, the Act explicitly exempts the State from the requirement of consent for the provision of services and licenses, a broad exception that can be extended to policing functions.
- **Purpose Limitation and Data Minimization:** While the Act mandates that personal data be used only for the purpose for which it was collected, the broad purposes of "preventing and detecting crime" can be stretched to justify almost any data processing activity. The principle of data minimization is difficult to enforce against a state apparatus that argues more data leads to greater security.

3.3 The Absence of Robust Provisions on Automated Processing

The DPDP Act is conspicuously silent on the specific risks posed by automated decision-making,including profiling and predictive analytics. Unlike the European Union's General Data Protection Regulation (GDPR), which provides a right for individuals not to be subject to decisions based solely on automated processing, the Indian Act contains no such safeguard. In a predictive policing context, this means an individual or an entire community could be flagged as a "potential criminal" by an algorithm without any human review, explanation, or recourse. This lack of a "right to explanation" is a critical democratic deficit.

4. The Puttaswamy Gap: Proportionality and the DPDP Act

The Supreme Court in Puttaswamy established a four-pronged test for any privacy infringement:

1. The action must be sanctioned by law.
2. It must pursue a legitimate state aim.
3. It must be proportionate to the object sought to be achieved.
4. There must be procedural guarantees against abuse of such interference.

The DPDP Act, particularly through Section 17, fails to meet this standard. The exemption clause is the law itself

sanctioning a potential violation without ensuring the other three prongs. It does not inherently require a proportionality assessment for each instance of surveillance. The Act lacks the procedural guarantees-such as prior judicial or independent oversight, transparency mandates for algorithms, and periodic review-that are essential to prevent abuse.

5. Recommendations for a Rights-Centric Framework

To align the use of predictive policing and AI surveillance with constitutional values, the following measures are imperative:

1. **Legislative Amendment:** The blanket exemption under Section 17 must be replaced with a specific, narrowly tailored regime for law enforcement data processing. This regime should incorporate the Puttaswamy proportionality standard directly into the text of the law.
2. **Regulatory Vigilance by the Data Protection Board (DPB):** The DPB must assert its authority to scrutinize state data processing activities that fall outside the exemption. It should issue guidelines on the use of FRT and predictive algorithms, mandating Data Protection Impact Assessments (DPIAs) for high-risk processing by the state.
3. **Introduction of Rights against Automated Decision-Making:** The Act should be amended to incorporate a right to meaningful human review and an explanation for decisions made solely by automated systems that have a significant legal or similar effect on individuals.
4. **Robust Oversight Mechanism:** An independent, multi-stakeholder oversight body, potentially with judicial members, should be established to authorize and review the use of intrusive surveillance technologies, moving beyond the current model of executive self-authorization.
5. **Transparency and Accountability:** Police departments using predictive models must be mandated to publicly disclose the basic nature of the technology, the data sources used, and the mechanisms in place to audit for bias and accuracy.

6. Conclusion

The Digital Personal Data Protection Act, 2023, marks a historic step towards recognizing data privacy in India. However, as a legal instrument designed to curb the excesses of state surveillance and algorithmic governance, it is fundamentally inadequate. Its broad exemptions for the state, coupled with the lack of specific safeguards against automated profiling, create a dangerous loophole that can legitimize a panopticon state. The promise of efficient, data-driven policing must not come at the cost of eroding the fundamental right to privacy and fostering a culture of suspicion and discrimination. For the DPDP Act to be a true guardian of citizens' rights, it must be interpreted and amended to ensure that the use of AI in policing is subject to the strict, proportionality-based scrutiny demanded by the Constitution. Without such corrective measures, the Act risks becoming a shield for the very intrusions it was meant to prevent.

7. References

1. Government of India. The Digital Personal Data Protection Act, 2023. Act No. 22 of 2023. New Delhi: Government of India; c2023.
2. Supreme Court of India. Justice K.S. Puttaswamy (Retd.) and Another vs. Union of India and Others. Writ Petition (Civil) No. 494 of 2012; c2017.
3. Barocas S, Selbst AD. Big data's disparate impact. California Law Review. 2016;104(3):671–732.
4. Bennett CJ, Raab CD. The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge (MA): MIT Press; c2006.
5. Ferguson AG. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York (NY): New York University Press; c2017.
6. Gupta A. The Indian surveillance state: a constitutional challenge. Indian Law Review. 2021;5(2):145–170.
7. Ramanathan U. The body in the database: Aadhaar and the citizen–non-citizen conundrum. Journal of Indian Law and Society. 2020;10(1):1–25.
8. Suresh K, Varma S. Predictive policing in India: a primer on the legal and ethical concerns. National Law School of India Review. 2022;34(1):89–115.
9. Centre for Internet and Society. Artificial Intelligence in India: A Policy Agenda. Bengaluru: Centre for Internet and Society; c2018.