AI REGULATIONS FOR THE STATE: FLEXIBLE OR INVASIVE?

Mudita Gupta, B.A. LL.B., Jindal Global Law School

ABSTRACT

As India rapidly adopts AI for State functions such as facial recognition, surveillance and predictive policing, the legal framework governing these technologies remains inadequate in terms of personal data protection. The new Digital Personal Data Protection Act of 2023 remains silent on the use of AI by the State in processing personal data. This paper's core concern lies in the broad exemptions provided by the Act to the State in the disguise of "certain legitimate uses." As per this, the Act allows government agencies to bypass fundamental notice and consent requirements in the name of sovereignty and public order. This leaves room for serious misuse and a large difference from the provisions the Act seeks to enforce on the private sectors, then from the public. Furthermore, the Act fails to provide citizens with any kind of redressal mechanisms against ambiguous algorithmic decisions, as a result of using FRT, predictive policing, etc. Finally, the paper presents recommendations to prevent these issues and to ensure that India's digital transformation does not come at the cost of fundamental rights.

Introduction

The Maha Kumbh Mela 2025 recorded over 3.4 million visitors on its quietest day and surged past 7.5 million on its most auspicious, all within a 40 square kilometre stretch of Prayagraj. To manage this scale, the Government of India deployed an extensive AI infrastructure across 2,760 CCTV cameras, facial recognition systems, drone monitoring, and real-time crowd analytics.[1] Sarita Singh, an attendee on one of these days was separated from her young son in the rush, authorities ran her son's photograph through their FRT. Within hours, a camera found him standing near a tea shop with his grandmother. The family was reunited.[2]

The promise of AI in State hands could not be more vivid. Yet India's only legislation governing digital personal data, the Digital Personal Data Protection Act, 2023, is entirely silent on the rules the State must follow when deploying AI surveillance of this kind. Where the Act does apply, it hands the State broad exemptions that could shield precisely these uses from scrutiny altogether. There is an urgent need for severe modifications in the DPDP Act to govern the consequences of AI use, especially by the State.

The Provisions of the DPDP Act, 2023

The DPDP Act is the appropriate focus for this paper because it is India's only statute explicitly governing digital personal data. A person's image or video captured by State surveillance cameras constitutes personal data within the Act's own definition, "data that identifies or is capable of identifying an individual."[3] No other operative statute, such as the IT Act, 2000, or any AI-specific regulation governs the processing of this data. The DPDP Act is therefore not merely an option among many, it is the only framework available.

Section 7 of the DPDPA permits the State to process personal data without consent for "certain legitimate uses" including sovereignty, security, public order, and prevention of offences.[4] Section 17 (2) (b) exempts the State from the Act's obligations more broadly, meaning even the limited safeguards that do exist can by bypassed.[5] The determination of "legitimate use"

[1] Sudev Kiyada and others, 'India's Kumbh Mela: The World's Largest Religious Gathering' *Reuters* (26 May 2025).
[2] Saurabh Sharma and Tanvi Mehta, 'Tech-savvy Maha Kumbh: India Aims for Safer Religious Festival' *Reuters* (23 January 2025).
[3] Digital Personal Data Protection Act 2023, s 2(t).
[4] Digital Personal Data Protection Act 2023, s 7.S
[5] Digital Personal Data Protection Act 2023, s 17.

under Section 7 is entirely discretionary and unreviewable. Conversely, there are strict notice and consent requirements, purpose limitations, data minimisation, and accuracy obligations that apply to private data fiduciaries. Additionally, there is no independent regulatory oversight of State data processing established under the Act.

AI Specific Risks

In 2026, the risks of unregulated AI surveillance are not theoretical, they are real life possibilities. An aggravator of such risks is the "black box" problem where algorithmic decisions are opaque not only to those affected by them, but often to the system's own operators.[6] FRT, as deployed in the Maha Kumbh Mela, AI surveillance in Mumbai during Ganesh Visarjan and the use of predictive policing in Telangana are all reminders that when the State uses AI to process personal data, without any statutory framework, there is no mechanism to challenge, audit, or even understand the basis of an adverse decision.[7][8] This is similar to the concept of "coding elite" where IT personnel exercise unaccountable discretion in designing the algorithms that drive these systems.[9] Evidently, in India these risks are already materialising. In 2020, Delhi Police deployed FRT during the protests following the Citizenship Amendment Act, without any legal basis or independent oversight.[10] Function creep, the use of data collected for one purpose to serve another, and dirty data that encodes historical biases further compound the risk of discriminatory outcomes.[11] Without binding rules governing State AI use, each of these deployments occurs in a legal vacuum.[12]

One may argue that voluntary entry into a CCTV-monitored public space constitutes implied consent to surveillance. However accurate, this resolves only the question of initial collection and not what it follows. Consent to be filmed does not extend to indefinite data retention, algorithmic processing through FRT, or reuse for predictive policing. Section 6 and 8 of the

[6] Marc Schuilenburg and Melvin Soudijn, 'Big Data Policing: The Use of Big Data and Algorithms by the Netherlands Police' (2023) 17 Policing: A Journal of Policy and Practice paad061.
[7] 'AI Drones, CCTV Cams and 25,000 Mumbai Cops Make a Tech-heavy Ganpati Visarjan Plan' *The Times of India* (Mumbai, 16 September 2024).
[8] VB Malleswari and Anjali Dixit, 'AI Integration in Telangana Police: Analyzing Efficiency and Ethical Dimensions' (2024) 28(1) Naturalista Campano 3374.
[9] Jenna Burrell and Marion Fourcade, 'The Society of Algorithms' (2021) 47 Annual Review of Sociology 213.
[10] 'Is the Illegal Use of Facial Recognition Technology by the Delhi Police Akin to Mass Surveillance? You Decide! #ProjectPanoptic' (Internet Freedom Foundation, 23 February 2021).
[11] Bert-Jaap Koops, 'The Concept of Function Creep' (2021) 13(1) Law, Innovation and Technology 29.
[12] Shveta Shokeen and Garima Sharma, 'Impact of Artificial Intelligence on Policing in India' (2024) 11(1) International Journal of Enhanced Research in Educational Development 1.

DPDP Act impose purpose limitation and data minimisation on private data fiduciaries.[13] The State, by virtue of Section 17(2)(b), is exempt from these obligations entirely. There is no statutory limit on how long the State retains surveillance data, who may access it, or for what secondary purpose it may be used. Implied consent at the beginning cannot be extended to authorise an unconstrained data lifecycle.

The Right to Privacy under Article 21

The DPDP Act's State exemptions do not merely reflect poor legislative drafting, they also raise a constitutional problem. In Justice K.S. Puttaswamy v. Union of India (2017), a nine-judge bench of the Supreme Court of India unanimously held that privacy is a fundamental right under Article 21, and that any State invasion of privacy must satisfy a four part proportionality test: there must be a legitimate aim, a rational connection between the aim and the measure, necessity (no less restrictive alternate exists) and a fair balance between ights infringed and the aim pursued.[14][15] The DPDP Act's exemptions do not strictly comply with these requirements. Section 7's "certain legitimate uses" are vague and unreviewable, there is no necessity threshold, and no balancing mechanism. The arbitrariness of the Act threatens constitutional safeguards.

Comparing EU Laws

The European Union's AI Act 2024 classifies real-time facial recognition in public spaces as a prohibited practice and categorises predictive policing tools as high-risk AI systems, mandating conformity assessments, human oversight, and transparency obligations before deployment.[16] Crucially, these restrictions apply to public authorities as much as private actors, meaning that the State receives no wholesale exemption. The GDPR, which played a significant role in drafting the DPDP Act, similarly binds government entities to the same data protection standards as private organisations.[17] At the international level, the Council of Europe's Framework Convention on Artificial Intelligence, explicitly requires signatory parties to ensure that AI systems deployed by public authorities respect human rights, democracy, and the rule

[13] Digital Personal Data Protection Act 2023, ss 6, 8.
[14] *Justice KS Puttaswamy (Retd) v Union of India* [2017] 10 SCR 569, (2017) 10 SCC 1
[15] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins 2019).
[16] AI Act or Regulation 2024/1689.
[17] GDPR or Regulation 2016/679.

of law.[18] India, which also deploys FRT, has no equivalent binding framework governing State AI use.

Recommendations

Three targeted reforms would address the DPDP Act's structural deficiencies. First, "certain legitimate uses" under Section 7 must be replaced with an exhaustive, narrowly defined list of permissible State purposes, accompanied by clauses requiring Parliamentary review at fixed intervals. Open-ended discretion is incompatible with the proportionality standard mandated by the Puttaswamy judgement. Second, algorithmic impact assessments must be mandated before any State deployment of AI in high-risk domains such as FRT, predictive policing, and automated decision-making affecting individual rights, modelled on the EU AI Act's conformity assessment framework. Third, the Data Protection Board's jurisdiction must be explicitly extended to State actors, with an accessible and independent complaints mechanism for citizens adversely affected by automated decisions. Taken together, these reforms would not eliminate legitimate State use of AI, instead they would ensure it operates within constitutional limits, subject to oversight, and with meaningful and accessible redress.

Conclusion

AI driven governance is not inherently dangerous, and Sarita Singh's story proves that. Deployed responsibly, these technologies can save lives, manage scale, and strengthen public administration in a country of 1.4 billion people with a rapidly expanding digital infrastructure. The question this paper asks is not whether the State should use AI, but whether it should do so without accountability. The answer, as per the landmark Puttaswamy judgement, is simply no. India's digital transformation is already underway. The surveillance infrastructure exists, the deployments are happening, and the legal framework has not kept pace. Correcting that gap does not require slowing down technological adoption. It requires ensuring that when the State looks for someone through its cameras next, it does so within constitutional limits, subject to oversight, and answerable to the people it serves.

[18] CoE AI Framework Convention.