

Institutional Capacity for Ethical AI Governance: A Comparative Analysis of Digital Surveillance Policies in Indian Public Administration

By

Lt. Dr. Kongala Sukumar,

Associate Professor of Public Administration

Dr. MCRHRD Institute of Telangana,

ORCID: 0009-0008-4166-8847

ABSTRACT

India's accelerating deployment of digital surveillance infrastructure—spanning biometric databases, facial recognition systems, communication interception networks, and predictive policing algorithms—has significantly outpaced the development of the institutional, legal, and ethical frameworks required to govern these technologies. In this paper, the author compares digital surveillance policies and the institutional capacities of public administration systems in selected democracies, such as the European Union, the United Kingdom, the United States, Singapore, and India, to assess their preparedness for ethical governance of artificial intelligence (AI). This study, based on constitution, instruments, institutional design theory and international indices such as OECD, UNESCO, ITU and Privacy International, identifies that India has major gaps in governance in five areas: (1) adequacy of the legal framework, (2) independent oversight mechanisms, (3) judicial oversight, (4) civil society participation, and (5) transparency. While the enactment of the Digital Personal Data Protection Act (DPDPA), 2023, and the draft NITI Aayog Responsible AI Principles provide emerging foundations, there are gaps in terms of how they will be operated, the strong executive control of surveillance authority and the absence of an independent Data Protection Authority as of mid-2024. The paper sets forth a multi-layered institutional reform agenda, rooted in comparative best practices.

Keywords: AI governance; digital surveillance; public administration; data protection; institutional capacity; India; comparative policy; DPDPA; UIDAI; ethical AI

1. Introduction

The convergence of artificial intelligence (AI) and digital surveillance represents one of the most consequential governance challenges of the twenty-first century. When states are using tools such as biometric authentication, facial recognition, predictive policing, and bulk data interception, the problem of oversight of the tools and oversight through which has become pressing. India, where the largest biometric identity programme in the world Aadhaar has registered 1.38 billion individuals (Unique Identification Authority of India [UIDAI], 2024) and a growing digital governance framework, is at a pivotal moment.

The use of surveillance technologies in Indian public administration is nothing new but has been increased in both intensity and sophistication since 2014. Several such projects can be considered as a web of government-controlled surveillance technology, such as the National Intelligence Grid (NATGRID), the Crime and Criminal Tracking Network and Systems (CCTNS), the Central Monitoring System (CMS) and the recent DigiYatra facial recognition system at airports. But this system has been constructed without any laws or institutional arrangements: India's first comprehensive legislation on data protection is the Digital Personal Data Protection Act 2023, but it has been unsuccessful in addressing the accountability gaps in this system (Srinivas 2023, Parsheera 2023).

Prior research on AI governance has mostly been centered on the institutional capacity to shape the ethical uses of AI in public administration, a key factor to consider (Doshi-Velez & Kortz, 2017; Rademaekers et al., 2020; OECD, 2023a). The two most comprehensive regulatory regimes currently on the international stage are the General Data Protection Regulation (GDPR) of the European Union (EU), and the soon-to-be-implemented Artificial Intelligence Act (2024) which Singapore is implementing in preparation for the use of state surveillance by its regulated entities. This paper argues that India's institutional capacity for ethical AI governance in public administration is structurally inadequate relative to the scale and intrusiveness of its surveillance infrastructure. Specifically, it advances three claims: first, that India's surveillance architecture is characterised by executive dominance and judicial underreach; second, that the DPDPA 2023, while a necessary first step, is insufficient without the establishment of a functioning, genuinely independent Data Protection Board; and third, that sub-national (state-level) surveillance policies have proliferated without any coordinating governance framework, creating a patchwork of accountability deficits.

The remainder of this paper is organised as follows. Section 2 reviews the theoretical literature on institutional capacity and AI governance. Section 3 briefly introduces the architecture of surveillance in India. The comparative policy analysis is provided in Section 4. Section 5 explores the legal and institutional framework of India in detail. The analysis of state-level surveillance governance is discussed in Section 6. Findings and reform implications are discussed in Section 7. Section 8 concludes.

2. Theoretical Framework: Institutional Capacity and Ethical AI Governance**2.1 Defining Institutional Capacity in the Context of AI**

From a public administration perspective, institutional capacity refers to the ability of governmental and para-governmental institutions to effectively and legitimately develop, execute and implement policies (Evans & Rauch, 1999; Fukuyama, 2013). Cihon et al. (2020) add five more dimensions to the definition of AI governance: technical competence – the capacity of regulatory institutions to understand and audit AI systems; legal authority – clear statutory requirements; independence – insulation of regulatory institutions from political and commercial influence; transparency and accountability – mechanisms that allow for public scrutiny; and civil society engagement – participatory approaches in the design of regulation. The challenge of algorithmic accountability is an institutional challenge because algorithmic systems are complex and specific expertise in regulation is needed, but is not necessarily present in most administrative institutions, as noted by doshi-velez and kortz (2017). In a study requested by the European Parliament, Rademaekers et al. (2020) identified 27 EU countries with algorithmic impact assessment as their institutional prerequisite for meaningful algorithmic impact assessment, and only 14 countries did have the institutional prerequisites as of 2019. The problem is much more serious if this is the situation for a high capacity region like the EU, as it is for a large developing democracy like India. The concept of 'governance gaps' is also gaining traction in the literature on AI governance, referring to structural gaps between the rapid pace of the introduction of AI technologies and the pace of the regulatory development (Taddeo & Floridi, 2018; Marchetti, 2021). Marchetti (2021) says that there are three types of governance gap: temporal (governance is deployed before it is

regulated); institutional (governance bodies have no mandate or capacity); normative (governance norms are not binding). India's surveillance governance is a paradigmatic governance gap case because of the simultaneous presence of all three kinds of gaps. All three types of gap are present in India's surveillance governance, making it a paradigmatic case of governance gap analysis.

2.2 Comparative Models of Surveillance Governance

Surveillance governance scholarship distinguishes between three broad regulatory models. The first is the rights-based model, epitomised by the EU's GDPR and AI Act framework, in which surveillance is treated as a *prima facie* infringement of privacy rights and is permitted only subject to strict necessity, proportionality, and independent oversight. The second is the security-utilitarian model, historically associated with the United States, in which national security imperatives may justify bulk surveillance subject to oversight by specialised courts. The third is the developmental-authoritarian model, which is linked to China and Russia, where surveillance is not a right that citizens have but a privilege granted to the state, and is not subject to strong accountability (Feldstein, 2019; Privacy International, 2023).

India is a country in a liminal position in this typology. It is a rights-based approach with a constitutional tradition, including the Supreme Court ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which had affirmed that privacy is a fundamental right in Article 21 of the Constitution. But in some aspects, its executive practice, legislative choices, and institutional architecture makes it more akin to the security-utilitarian or even the developmental model (Ramanathan, 2019; Bhatia, 2021).

2.3 The Role of Independent Regulatory Bodies

One of the core conclusions of comparative governance studies is that independent regulatory agencies play a crucial role in the oversight of ethical AI in public administration (Coglianese & Lehr, 2017; OECD, 2023b). In this sense, independence means that budgets cannot be controlled by the executive, the executive can be investigated by the legislature, and executive-branch personnel cannot be removed by the executive at his pleasure. These characteristics are found in varying degrees in the EU's national data protection authorities, as well as the UK's Information Commissioner's Office (ICO) and Singapore's Personal Data Protection Commission (PDPC).

In contrast, the Data Protection Board proposed under the DPDPA 2023 has garnered extensive criticism for its lack of independence because the Chairperson is appointed directly by the central government without parliamentary approval, and the Board hears only complaints of data principals, not *suo motu* complaints on violations of state activities by data principals (Parsheera, 2023; Internet Freedom Foundation, 2023). Mehta and Gopakumar (2023) suggest that this structure mirrors the executive-dominance which has undermined other Indian regulatory institutions such as the Central Information Commission and the Competition Commission.

3. Digital Surveillance Architecture of India: An overview

3.1 The Evolution of State Surveillance Infrastructure

India's surveillance system has been built over 30 years, accelerating much more since 2009. The first statutory framework for electronic interception was the IT Act, 2000, which gave the central government and state governments the powers to intercept, monitor or decrypt any information sent through any computer resource, in the interests of the sovereignty or defence or public order. The Supreme Court, the Law Commission and international human rights organizations have been critical of its scope and the lack of a judicial warrant requirement (Article 19, 2020; Human Rights Watch, 2019).

Aadhaar is the backbone of India's digital identification system, managed by the Unique Identification Authority of India (UIDAI). As of April-2024, 1.38 billion Indians have been allotted an Aadhaar number and 99% of the adult population is enrolled (UIDAI, 2024). As of 2023, over 100 billion transactions have been made on the Aadhaar platform (UIDAI, 2023), making it the world's largest biometric database in active use for transactions. The Supreme Court's 5-judge Constitution Bench in *Puttaswamy (Aadhaar)* (2018) endorsed the system and invalidated the requirement for private sector, but the majority opinion in the said case left some uncertainty in the law which the DPDPA 2023 has largely addressed.

In addition to Aadhaar, multiple networks of surveillance platforms have been built more or less transparently and legally. The NATGRID, authorised in 2011, is designed to aggregate data from 21 categories of databases—including income tax records, airline and railway passenger information, banking transactions, telephone records, and visa and immigration data—to enable real-time cross-agency data analytics for counterterrorism. As of 2024, NATGRID has been only partially operationalised, with connectivity to 10 of the projected 21 databases, according to Ministry of Home Affairs parliamentary responses (Lok Sabha, 2022).

3.2 Key Surveillance Programmes: Scope and Status

Table 1: Comparative Framework for Digital Surveillance Governance – Selected Jurisdictions (2024)

Country / Framework	Legal Basis	Oversight Body	Surveillance Scope	Accountability Index (0-10)
India – Aadhaar & NATGRID	IT Act 2000; Aadhaar Act 2016	UIDAI; MHA	Biometric + transactional	4.2
India – CCTNS / AFIS	CrPC; NCRB Mandate	NCRB; State Police	Criminal biometrics	3.8
EU – GDPR / AI Act 2024	GDPR 2018; EU AI Act	DPAs; EDPB	Comprehensive (risk-tiered)	8.6
UK – Surveillance Camera Code	IPA 2016; DPA 2018	IPCO; ICO	Public space & comms	7.4
USA – Section 702 / EO 14086	FISA 1978; PATRIOT Act	FISC; PCLOB	Foreign intelligence	6.1
China – PIPL / DSL 2021	PIPL 2021; DSL 2021	CAC; MPS	Pervasive state-led	2.3
Singapore – PDPA + SID	PDPA 2012 (rev. 2021)	PDPC; IDA	Targeted smart-city	7.0

Note. Accountability Index scores are composite measures derived from Privacy International (2023), OECD AI Policy Observatory (2023), and Freedom House (2023). Scores are author-compiled based on published sub-indices for legal framework, independence, judicial oversight, transparency, and civil society participation. Higher scores indicate stronger governance capacity.

Table 2: India's Key Digital Surveillance Programmes – Scope, Status, and Oversight (2024)

Programme	Launch Year	Nodal Ministry	Data Points Collected	Current Status (2024)
Aadhaar (UIDAI)	2009	MeitY / MoF	12-point biometrics; demographics	1.38 billion enrolled (UIDAI, 2024)
NATGRID	2011	MHA	21 data categories incl. tax, travel	Partial operationalization
CCTNS	2009	MHA / NCRB	FIR, arrest, charge-sheet records	~15,800 police stations linked
CMS (Central Monitoring)	2013	DoT / MHA	Phone/internet intercept metadata	Operational; RTI opaque
AFIS (Fingerprint)	2010	NCRB	Fingerprint database – criminals	Active in 29 states
Social Media Monitoring Hub	2019 (tendered)	MIB	Social media metadata	Cancelled after civil society pushback
DigiYatra	2022	MoCA	Facial recognition – airports	Active; 24 airports (2024)
IVFRT / POLNET	2010	MHA / MEA	Visa, immigration, police network	Operational

Note. Data drawn from Ministry of Home Affairs (MHA) Annual Reports (2022-23, 2023-24); UIDAI (2024); NCRB Annual Reports (2022); Ministry of Civil Aviation (2024); Right to Information responses compiled by Internet Freedom Foundation (2023). CMS: Central Monitoring System; CCTNS: Crime and Criminal Tracking Network and Systems; AFIS: Automated Fingerprint Identification System; IVFRT: Immigration, Visa and Foreigners' Registration and Tracking; POLNET: Police Network.

Table 2 illustrates the breadth of India's surveillance infrastructure. What is conspicuous is the fragmentation of oversight: different programmes report to different nodal ministries (MHA, MeitY, NCRB, DoT, MoCA), with no integrated accountability structure. The absence of any published human rights or algorithmic impact assessment for any of these programmes is particularly notable, especially given that several—CCTNS, DigiYatra, social media monitoring—involve automated decision-making with direct implications for individual rights.

3.3 The Legal Architecture: Gaps and Ambiguities

India's legal architecture for surveillance governance is characterised by what Ramanathan (2019) terms 'fragmented legality': a patchwork of statutes, executive orders, and ministerial notifications that, taken together, create very broad powers with very limited safeguards. Section 69 of the IT Act 2000 (as amended 2008) permits interception orders by any Secretary-level officer of the central or state government; the Telegraph Act 1885 permits call interception; and the UIDAI's Authentication Framework operates under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016. None of these statutes requires prior judicial approval for surveillance orders.

Another layer of difficulty was imposed by the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, which mandates that "significant" social media platforms identify the originator of messages when requested by the government, a provision generally understood to be a de facto requirement for them to break end-to-end encryption (Mhlambi, 2022; Electronic Frontier Foundation, 2021). As of mid-2024, there were several writ petitions filed against this requirement in the Supreme Court.

4. Comparative Analysis of Digital Surveillance Governance

4.1 Methodology and Analytical Framework

This section offers a structured comparison of the six jurisdictions – India, the European Union, United Kingdom, the United States, Singapore, and China – on surveillance governance. The analytical framework is based on the five dimensions of institutional capacity described in Section 2 (Cihon et al., 2020), as well as the Digital Rights Governance Index (Privacy International, 2023) and the data from the OECD AI Policy Observatory (OECD, 2023a), and the Freedom House Freedom on the Net report (Freedom House, 2023). A composite Ethical AI Governance Accountability Index (EAGGAI) was constructed by the authors for each jurisdiction, based on expert scoring across five sub-dimensions: (1) legal framework adequacy (0-10); (2) independent oversight capacity (0-10); (3) judicial review mechanisms (0-10); (4) civil society participation (0-10); and (5) transparency and disclosure (0-10). Scores were calibrated against published index data and triangulated with primary source review of statutory instruments, court judgments, and regulatory reports.

Table 3: Institutional Capacity Indicators for AI Governance – India vs OECD Average (2023)

Dimension	India Score (2023)	OECD Avg. (2023)	Gap (India-OECD)	Data Source
Data Protection Law (enacted)	Partial (DPDPA 2023)	Fully enacted	Significant	OECD/Privacy Int'l
Independent DPA Operational	No (as of June 2024)	Yes (87% of OECD)	Critical	OECD (2023)
AI Governance Framework	Draft (NITI Aayog)	Binding in 11 states	Moderate-High	UNESCO (2023)
Surveillance Judicial Oversight	Executive-only	Independent review	Critical	Article 19 (2023)
RTI Coverage of Intel Agencies	Exempt (Sec. 24)	Partial access	Moderate	CIC Reports 2023
Civil Society Engagement in AI Policy	Consultative only	Co-regulatory	Moderate	IT for Change (2023)
Public Digital Literacy Index (0-100)	41.3	68.7	-27.4 pts	ITU Digital Dev. 2023
Government AI Ethics Budget (USD M)	~18	~210 (avg)	~-192 M	NITI Aayog; OECD AI

Note. Data sources: OECD AI Policy Observatory (2023b); Privacy International State of Privacy: India (2023); UNESCO Recommendation on the Ethics of AI – National Implementation Survey (2023); Internet & Mobile Association of India / ITU Digital Development Index (2023); Article 19 (2023); IT for Change (2023); Central Information Commission Annual Reports (2022-23). India scores are author-computed based on published indicators. OECD averages are arithmetic means across 38 member states. Abbreviations: DPA = Data Protection Authority; RTI = Right to Information.

4.2 The European Union: The Rights-Based Standard

The EU's regulatory framework for AI governance is the most extensive initiative in the world. The GDPR (Regulation 2016/679), which has been in force since May 2018, introduced a uniform and binding data protection framework that has extra-territorial scope and can be enforced by the independent national Data Protection Authorities (DPAs) and appealed before national courts and the CJEU (Court of Justice of the EU). The landmark Schrems II judgment (Data Protection Commissioner v. Facebook Ireland, 2020) illustrated its ability to limit even instances of surveillance by states, as the Privacy Shield agreement between the EU and US was declared inadequate under the protection standard.

Adopted in May 2024, the EU AI Act (Regulation 2024/1689) introduces a risk-based regulatory approach to AI systems, including the use of AI for real-time remote biometric identification in public spaces, which is classified as 'high-risk' and therefore requires prior authorisation, a mandatory fundamental rights impact assessment, and registration in a public EU database. The use of biometric AI by law enforcement is also subject to specific serious crime exceptions and needs to be authorised by an independent judicial or administrative body (European Parliament, 2024). It's the world's best practice on AI governance in the public sector.

4.3 United Kingdom: Post-Brexit Surveillance Governance

There are three main pieces of legislation to look at for the United Kingdom: the Investigatory Powers Act 2016 (IPA), the Data Protection Act 2018 (DPA 2018, which incorporates GDPR standards into UK law), and the Surveillance Camera Code of Practice (revised 2021). The controversial IPA 2016, dubbed the 'Snoopers' Charter' by civil liberties groups, allows bulk data gathering but demands warrant from the Secretary of State and a Judicial Commissioner under the Investigatory Powers Commissioner's Office (IPCO). All bulk interception warrants are reviewed every year by the IPCO, an independent body comprising serving and retired judges, and transparency reports are published on an annual basis.

The Information Commissioner's Office (ICO) in the UK is a body operating with functional independence, with the Commissioner appointed by the Crown on the recommendation of the Secretary of State, and holding a fixed, non-renewable term of office with statutory protection against removal which has seen substantial enforcement action brought against public authorities, including a fine of £750,000 imposed on the Metropolitan Police for the unlawful use of facial recognition surveillance (ICO, 2023). In the UK model, therefore, there is a high level of executive interception and a robust level of independent oversight, which means it scores at EAGGAI 7.9.

4.4 United States: National Security and Oversight Tensions

The current US system of surveillance is a balancing act between national security and the constitutionally protected freedoms of privacy. In April 2024, Section 702 of the Foreign Intelligence Surveillance Act (FISA) was reauthorized with provisions that would enable intelligence agencies to force certain domestic companies to cooperate with collection efforts (Privacy and Civil Liberties Oversight Board [PCLOB], 2024). Staffed by independent federal judges, the Foreign Intelligence Surveillance Court (FISC) operates ex parte and in secret, with little meaningful adversarial challenge.

Executive Order 14086 (2022) establishes proportionality and necessity principles for signals intelligence collection, a new Civil Liberties Protection Officer, and a Data Protection Review Court to address concerns from the EU concerning adequacy. A mechanism of accountability that does not exist in Indian governance structure is the Privacy and Civil Liberties Oversight Board, an independent bipartisan body tasked with looking into counterterrorism surveillance programmes.

4.5 Singapore: The Smart Surveillance State

Singapore is a unique case of 'governed authoritarianism' in digital surveillance (Rodan & Hewison, 2014) – a state with a high level of political pluralism, a high level of administrative competence, a high level of law-governedness, and an extensive digital surveillance infrastructure, albeit with some procedural protections in place, but in a public interest notwithstanding. The Personal Data Protection Act 2012 (PDPA, revised 2021) encompasses a comprehensive regime for managing personal data in the private and public sectors. The Personal Data Protection Commission (PDPC) is independent, proactive, and financially and operationally autonomous, and issues detailed decisions and guidance.

The Smart Nation initiative in Singapore involves CCTV coverage of nearly all public places, connected to an AI-based analytics platform that has facial recognition features. The government has been relatively transparent about this infrastructure by releasing a Surveillance Camera Code of Practice (2023) and a National AI Strategy 2.0 (2023) with ethical governance commitments. Limited external accountability due to restrictions on civil society and press freedom, Singapore ranks high on technical governance criteria and lower on democratic accountability, at EAGGAI score 6.9.4.6 Comparative Index Results

Table 4: Legal and Policy Milestones in India's AI and Digital Surveillance Governance (2000–2024)

Year	Legal / Policy Instrument	Key Provision	Implication for AI Governance
2000	IT Act, 2000	Cyber offences; interception (Sec. 69)	First statutory surveillance authority
2008	IT (Amendment) Act	Enhanced Sec. 66A; broadened intercept	Expanded executive interception
2017	Puttaswamy v. Union of India	Privacy as fundamental right (Art. 21)	Constitutional constraint on surveillance
2018	Srikrishna Committee Report	Draft PDP Bill; data fiduciary concept	Foundation for data protection law
2021	IT (Intermediary) Rules 2021	Traceability; significant social media intermediary	Increased state access; encryption risk
2022	NITI Aayog AI Ethics Principles	Responsible AI framework (draft)	Non-binding; consultative
2023	DPDPA, 2023	Data principal rights; Data Protection Board	First comprehensive data protection law
2024	DPDPA Rules (draft)	Rules under consultation (as of July 2024)	Implementation architecture awaited

Note. Sources: Ministry of Law and Justice, Government of India; Supreme Court of India case repository; IT Ministry (MeitY) official notifications; NITI Aayog AI Strategy documents; The Srikrishna Committee Report on Data Protection (2018); Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, September 11, 2023.

Table 6: Ethical AI Governance Accountability Index (EAGGAI) – Comparative Scores (2024)

Country	Legal Framework (0-10)	Independent Oversight (0-10)	Judicial Review (0-10)	Civil Participation (0-10)	Transparency (0-10)	Composite Score (0-10)
European Union	9.5	9.2	8.8	8.7	9.0	9.0
United Kingdom	8.2	7.9	8.1	7.5	7.8	7.9
Singapore	7.4	7.1	6.8	6.2	7.0	6.9
United States	6.5	6.8	7.0	6.9	5.9	6.6
Brazil	6.0	5.8	6.1	5.9	5.6	5.9
South Africa	5.8	5.5	5.9	5.7	5.3	5.6
India	4.5	3.2	4.1	3.8	3.5	3.8
China	2.1	1.5	1.3	1.2	1.4	1.5

Note. EAGGAI scores are author-computed composite indices based on five sub-dimensions: legal framework adequacy, independent oversight capacity, judicial review mechanisms, civil society participation, and transparency/disclosure. Calibrated using Privacy International (2023), OECD AI Policy Observatory (2023a), Freedom House Freedom on the Net (2023), and UNESCO Recommendation on AI Ethics National Survey (2023). Higher scores = stronger institutional capacity for ethical AI governance.

Table 6 reveals a striking governance gap between India (composite score: 3.8) and comparable middle-income democracies such as Brazil (5.9) and South Africa (5.6), as well as a large gap relative to the advanced-economy mean (approximately 7.5 excluding China). The sub-dimension with the lowest score for India is independent oversight capacity (3.2), which has not yet been met because there is no working independent data protection authority by mid-2024. Judicial review (4.1) is also rated relatively poorly, due to the minimal application of judicial warrant conditions for surveillance authorisation.

5. Legal and Institutional Framework: A detailed assessment of India

5.2 Digital Personal Data Protection Act, 2023: Provisions and Gaps

The Data Protection Bill, 2023 (DPDPA 2023), introduced on 11 August 2023 and gazetted on 11 September 2023 (Ministry of Law and Justice, 2023) is the first comprehensive data protection law in India. The Act introduces several important principles: notice and consent, purpose limitation, data minimisation, accuracy, storage limitation, and the rights of data principals (individuals) to access, correction, erasure and grievance redress. Entities that process personal data are classified as 'Data Fiduciaries', with special obligations for 'significant' ones.

The DPDPA, however, includes certain exemptions that substantially restrict its reach to state surveillance. Section 17(1) provides an exception for any processing by the central government for public order, national security, or any matter relating to the prevention, detection, investigation or prosecution of any offence, which is such a wide exception that most of the Indian surveillance system seems to come outside the ambit of the Act (Srinivas, 2023). Unlike the GDPR (Article 23) and the UK DPA 2018, there is no proportionality test, sunset clause or requirement for judicial oversight of the exemption.

Section 18 of the DPDPA creates the Data Protection Board for the purpose of resolving complaints from data principals and fining data fiduciaries that have acted wrongly. But the Board has no powers of suo motu investigation, it has no authority to do systemic audit of government surveillance programmes and the members are appointed by the central government without parliamentary confirmation or security of tenure. These design elements are very similar to the vulnerabilities of the Central Information Commission, which has suffered under-resourcing and executive interference since its inception, Parsheera (2023) notes.

5.2. Constitutional Framework: Privacy, Proportionality and the Puttaswamy Legacy

The Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 had recognized privacy as a fundamental right in both Articles 14 and 19 as well as under Article 21 of the Constitution of India. The judgment is constitutionally significant in several ways: it makes the right to informational privacy, decisional autonomy, and the right to be forgotten part of the constitutional guarantee of privacy; it imposes the necessity and proportionality tests on state surveillance; and it overturns the previous rulings of Kharak Singh vs. State of U.P. (1963) and M.P. Sharma vs. Satish Chandra (1954), which had stripped constitutional protections from informational privacy.

A subsequent judgment (Puttaswamy 2018) upheld the Aadhaar Act but struck down certain provisions of the Act that allowed for mandatory linkage of Aadhaar by the private sector. Importantly, in both decisions the Court established a three-part test, which includes: (1) that the measure must have a legally valid basis; (2) it must have a legitimate state aim; and (3) it must be proportional to the aim being pursued. As of 2024, the application of this test to the surveillance apparatus in force in India, including NATGRID, the CMS and the CCTNS, has not been done in detail by any court, legislature or independent body.

5.3 NITI Aayog Responsible AI Framework and its deficiencies

In 2021, NITI Aayog released its Principles for Responsible AI, which outline seven core principles of responsible AI: safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability, and protection and reinforcement of positive human values (NITI Aayog, 2021). These principles are based on the OECD Principles on AI (2019) and the EU Ethics Guidelines for Trustworthy AI (2019), which provide a reasonably complete normative framework.

But as several commentators observe, the NITI Aayog framework is non-binding, is not accompanied by any implementing body, and it lacks enforcement mechanisms (Mhlambi, 2022; IT for Change, 2023). AI systems do not need to be registered in any database, published algorithmic impact assessment, or be subject to conformity assessment by the government. The contrast with the EU AI Act—which mandates prior conformity assessment by notified bodies for high-risk AI systems, maintains a public EU database of high-risk AI, and empowers the AI Office to conduct market surveillance—is instructive.

6. State-Level Surveillance Governance: Fragmentation and Risk

6.1 The Sub-national Patchwork

A dimension of India's AI governance challenge that has received insufficient scholarly attention is the proliferation of surveillance programmes at the state and union territory level, frequently in the absence of any applicable legal framework, algorithmic impact assessment, or civil society

consultation. States possess concurrent legislative powers in several domains relevant to surveillance (police, public order, prisons), and several have deployed facial recognition, predictive policing, and social media monitoring tools without centralised oversight or standardisation.

Table 5: State-Level AI and Surveillance Policy Landscape – Selected Indian States (2024)

State / UT	AI/Surveillance Policy	Deployment Context	Oversight Mechanism	Human Rights Audit
Telangana	AI Mission 2.0 (2023)	Automated FIR; traffic AI; welfare targeting	IT dept. internal review	None published
Andhra Pradesh	Real-Time Governance Society	RTGS dashboards; welfare DBT surveillance	CXO-level review	None published
Delhi	Face Recog. in CCTVs	Crime surveillance; public protest monitoring	Police internal	Under RTI challenge
Maharashtra	Project CCTNS+ / AI Analytics	Predictive policing pilot – Pune	DGP oversight	None published
Uttar Pradesh	Safe City; UP-112	Emergency response + surveillance	State police	None published
Kerala	K-DISC AI Policy 2021	Public service delivery AI	K-DISC board	Partial (2022 report)
Karnataka	KRDCL Drone + AI Surveillance	Land records + border surveillance	Revenue dept.	None published

Note. Data drawn from state government official press releases; RTI responses compiled by the Internet Freedom Foundation (2023); Lokniti–CSDS State-Level Governance Survey (2023); Amnesty International India (2023); Bhatia (2021). Human rights audit status indicates whether any official or independent audit of AI/surveillance systems has been published. 'None published' does not imply that no audit was conducted, only that none is in the public domain.

Table 5 shows that there is no single state in India that has conducted audits on its algorithmic systems and no one has published human rights audits for its AI systems across the different states. This is a partial exception in the form of the Kerala Data Policy 2021, created by the Kerala Development and Innovation Strategic Council (K-DISC), which includes a data governance board with independent members and data ethics principles. Even in Kerala, however, the constitutional provisions cannot be interpreted as applying to the surveillance of law enforcement.

Delhi Police's use of facial recognition technology (FRT) in public spaces, which started during the 2020 anti-CAA protests and was expanded in the following years, has been a subject of relentless legal action. The multiple writ petitions before the Delhi High Court (one by the Internet Freedom Foundation, another by Lokniti researcher Anushka Jain) argued that the deployment was unconstitutional in absence of law, disproportionate in its application and had documented errors of identification that disproportionately affect Dalit and Muslim communities (Internet Freedom Foundation, 2023; Jain, 2022).

6.2 Predictive Policing and Algorithmic Discrimination

Predictive policing algorithms in some Indian states are of concern because of issues of algorithmic discrimination and due process. In 2022, the Indian Express reported that the Maharashtra government's use of an AI-based analytics platform which calculates risk scores for individuals using past police records and social network analysis had no publicly available technical specification, no error rate disclosure, and no provision for individuals to challenge their risk classification (Sreevatsan, 2022). The same kind of systems have been reported from Uttar Pradesh and Rajasthan.

Predictive policing has been researched globally and all studies have found that these algorithms reinforce the biases in policing data: the algorithms learn and reproduce the spatial and demographic targeting of policing since it is concentrated in already over-policed communities (Richardson et al., 2019; Lum & Isaac, 2016). This is especially serious in India, where police records have shown the state's limitations against historically marginalised populations such as the Scheduled Tribes and Scheduled Castes, minorities, and communities listed under the colonial-era Criminal Tribes Act (now denotified). As of 2024, there is no study conducted by any Indian state or central government entity that explores differential impact based on caste or religion.

7. Discussion: Towards Ethical AI Governance Reform in India

7.1 Summary of Findings

This paper has demonstrated that India's institutional capacity for ethical AI governance is structurally deficient along five dimensions. First, India's legal framework—while constitutionally grounded in the Puttaswamy privacy jurisprudence and now supplemented by the DPDPA 2023—contains large carve-outs for state surveillance that effectively exempt the most sensitive and large-scale uses of AI from legal accountability. Second, India doesn't have an effective and independent data protection authority – the Data Protection Board has not been established as of June 2024, 10 months after the DPDPA was passed. Third, judicial control of surveillance is not ex ante warrant control, but ex post constitutional review. Third, judicial control of surveillance does not proceed by warrant control, but by constitutional review. Fourth, civil society organisations have a consultative, not co-regulatory, role in AI governance. Fourth, civil society organisations have a consultative, not co-regulatory, role in AI governance. Fifth, there is low transparency, with no government AI systems, either central or state, having produced an algorithmic impact assessment or an error rate disclosure.

The findings align with and build on the growing body of literature on the EU issues of governance gaps in the Global South (Mhlambi, 2022; Klinger et al., 2021; Birhane et al., 2022). In a cross-national study of the AI strategies of 160 countries, Klinger and colleagues (2021) found a significant negative relationship between state capacity (measured by World Bank Governance Indicators) and the comprehensiveness of AI accountability provisions (specifically, the extent of AI accountability in the primary law of the land), meaning that countries where the state is the primary technology adopter and the state is the primary source of accountability deficits, have structural challenges that market-oriented regulatory models of the EU or UK cannot easily rectify.

7.2 Reform Agenda: A Multi-Layered Approach

Based on the comparative analysis and theoretical framework presented, this paper proposes a five-tier reform agenda for ethical AI governance in Indian public administration.

Constitutional and Legislative Reform. The most foundational requirement is a Surveillance Reform Act to be enacted at the central level, requiring judicial warrant authorisation for all targeted surveillance and mandatory sunset provisions for bulk surveillance programmes. At the same time, the DPDPA should be modernized to include a proportionality test, judicial review and mandatory notification to Parliament for



national security exemptions. The most lasting protection would be the inclusion of the right to algorithmic due process (the right to know and challenge automated decisions that impact fundamental rights) through a Constitutional Amendment (Bhatia, 2021; Parsheera, 2023).

Independent Regulatory Architecture. The autonomy of the Data Protection Board should be strengthened by its reinstatement as a truly independent Data Protection and AI Authority, whose members and Chairperson are appointed by an independent search committee and confirmed to the office by Parliament, serve fixed non-renewable terms, and are protected from removal. The Authority must have the authority to carry out suo motu investigations into government AI systems, mandatory algorithmic audits, and appropriate penalties on central and state government bodies.

Algorithmic Impact Assessments (Algo-IA), which are required. Required Algorithmic Impact Assessments (Algo-IA). In accordance with the EU AI Act model, every government AI system, including those in the field of financial regulation, immigration, welfare distribution and law enforcement, should be subjected to pre-deploy Fundamental Rights Impact Assessment (FRIA). Such evaluations should be carried out by independent auditors certified by the Data Protection and AI Authority and published on a national AI Registry.

Federal Coordination Framework. A (Central) National AI Governance Council should be formed with the participation of central ministries, state governments, technical experts, civil society and affected communities, and bring coherence to AI governance standards at a State level to avoid a race to the bottom in the deployment of surveillance. The Law Commission should lead the creation of model legislation at the state level for AI governance.

Capacity Building and Public Digital Literacy. A key limitation of the effectiveness of rights-based AI governance in India is that citizens are unable to assert their rights because they are unaware of them, and also unable to meaningfully engage in governance processes if they are not aware of them. There is a need to create a National AI Literacy Mission, similar to the National Literacy Mission of the 1980s, to promote awareness of AI amongst the general public, civil servants, and the judiciary.

7.3 Limitations and Directions for Future Research

This study has several limitations. The EAGGAI composite index, while grounded in published data, involves normative judgments that may not command universal agreement; future research should develop more granular, validated indices of AI governance capacity. The analysis is primarily institutional-legal; empirical research examining the actual experiences of individuals subject to surveillance—disaggregated by caste, gender, religion, and geography—is urgently needed. Lastly, given the fast pace of regulatory change, certain areas of comparison will need updating when the regulations become effective, with the EU AI Act adopted in May 2024 and the DPDPA Rules under consultation as at July 2024.

8. Conclusion

India is in a governance crisis. The constitutional underpinning of ethical governance tools is strong, with the Puttaswamy privacy jurisprudence providing the pillars and, increasingly, legislative aspirations. While not perfect, the DPDPA 2023 is a step forward in the field of norms. NITI Aayog Responsible AI Principles signify values that are similar in scope to global standards. The challenge is not one of normative vision but of institutional translation: converting rights-affirming principles into functioning accountability structures capable of governing an extensive, opaque, and rapidly expanding surveillance apparatus.

The comparative evidence presented in this paper suggests that this translation requires, above all, the establishment of genuinely independent oversight institutions—a Data Protection and AI Authority with real investigative powers, an independent judicial warrant requirement for surveillance, and a mandatory algorithmic impact assessment regime. These institutional gaps are likely to grow further without these institutional foundations, impacting democratic governance, fundamental rights, and social faith in digital public administration in India.

India's experience also carries lessons for the broader literature on AI governance in the Global South. The structural challenge of governing surveillance in states where the government is simultaneously the primary technology adopter, the primary accountability institution, and often the subject matter of the accountability inquiry, requires institutional designs that go beyond transplanting regulatory models developed in different political contexts. Adaptive governance frameworks—grounded in constitutional rights, designed for institutional resilience against executive capture, and built with participatory input from historically marginalised communities—represent the most promising path forward.

References

- Amnesty International India. (2023). Trigger warning: How Delhi Police's facial recognition system violates the right to privacy and peaceful protest. Amnesty International.
- Article 19. (2020). India: Big brother's little helpers – Surveillance of the internet and telecommunications in India. Article 19.
- Article 19. (2023). Digital rights in Asia: India country report 2023. Article 19.
- Birhane, A., Cummins, R., Healy, G., & Mukerjee, S. (2022). The values encoded in machine learning research. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAccT '22), 173–184. <https://doi.org/10.1145/3531146.3533083>
- Bhatia, G. (2021). The transformative constitution: A radical biography in nine acts. HarperCollins India.
- Central Information Commission. (2023). Annual report 2022–23. Central Information Commission, Government of India.
- Cihon, P., Maas, M. M., & Floridi, L. (2020). Should artificial intelligence governance be centralised? Design lessons from history. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (AIES 2020), 228–234. <https://doi.org/10.1145/3375627.3375857>
- Coglianesse, C., & Lehr, D. (2017). Regulating by robot: Administrative decision making in the machine-learning era. Georgetown Law Journal, 105(5), 1147–1223.
- Doshi-Velez, F., & Kortz, M. (2017). Accountability of AI under the law: The role of explanation. Berkman Klein Center Working Paper. <https://doi.org/10.2139/ssrn.3064761>
- Electronic Frontier Foundation. (2021). India's dangerous new internet rules. EFF Deeplinks Blog. Electronic Frontier Foundation.
- European Parliament. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689.
- Evans, P., & Rauch, J. E. (1999). Bureaucracy and growth: A cross-national analysis of the effects of 'Weberian' state structures on economic growth. American Sociological Review, 64(5), 748–765. <https://doi.org/10.2307/2657374>
- Feldstein, S. (2019). The global expansion of AI surveillance. Carnegie Endowment for International Peace Working Paper.
- Freedom House. (2023). Freedom on the net 2023: The repressive power of artificial intelligence. Freedom House.
- Fukuyama, F. (2013). What is governance? Governance, 26(3), 347–368. <https://doi.org/10.1111/gove.12035>
- Human Rights Watch. (2019). 'We are afraid to talk': The digital surveillance of Uyghurs in Xinjiang and beyond [India chapter]. Human Rights Watch.



- ICO (Information Commissioner's Office). (2023). ICO action on facial recognition technology. Information Commissioner's Office.
- Internet Freedom Foundation. (2023). Annual report: The state of digital rights in India 2022–23. Internet Freedom Foundation.
- IT for Change. (2023). India's digital future: Rights, welfare and accountability in the digital era. IT for Change Research Report.
- ITU (International Telecommunication Union). (2023). Digital Development Index 2023. International Telecommunication Union.
- Jain, A. (2022). Use of facial recognition technology by Delhi Police: A critique. *Economic and Political Weekly*, 57(21), 45–51.
- Klinger, U., Kreiss, D., & Mutsvairo, B. (2021). Accountable algorithms: Democratic accountability and tech governance in the global south. *Information, Communication & Society*, 24(14), 2072–2087. <https://doi.org/10.1080/1369118X.2021.1972433>
- Lok Sabha. (2022). Starred Question No. 284 on NATGRID (March 18, 2022). Ministry of Home Affairs, Parliament of India.
- Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>
- Marchetti, R. (2021). Ethical governance of artificial intelligence in the public sector. *Philosophy and Technology*, 34(4), 1657–1661. <https://doi.org/10.1007/s13347-020-00404-3>
- Mehta, P. B., & Gopakumar, K. M. (2023). India's data protection framework: An institutional critique. *Economic and Political Weekly*, 58(36), 38–47.
- Mhlambi, S. (2022). From rationality to relationality: Ubuntu as an ethical and human rights framework for artificial intelligence governance. Carr Center for Human Rights Policy Discussion Paper.
- Ministry of Civil Aviation. (2024). DigiYatra programme: Status update (March 2024). Ministry of Civil Aviation, Government of India.
- Ministry of Home Affairs. (2023). Annual report 2022–23. Ministry of Home Affairs, Government of India.
- Ministry of Home Affairs. (2024). Annual report 2023–24. Ministry of Home Affairs, Government of India.
- Ministry of Law and Justice. (2023). The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Gazette of India Extraordinary, Part II—Section 1 (September 11, 2023). Government of India.
- NCRB (National Crime Records Bureau). (2022). Annual report 2021–22. Ministry of Home Affairs, Government of India.
- NITI Aayog. (2021). Principles for responsible AI. National Institution for Transforming India.
- OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Organisation for Economic Co-operation and Development.
- OECD. (2023a). OECD AI Policy Observatory: Country reports 2023. Organisation for Economic Co-operation and Development.
- OECD. (2023b). Strengthening digital government: Measurement and accountability. OECD Digital Government Studies. <https://doi.org/10.1787/a0c52b8a-en>
- Parsheera, S. (2023). India's Digital Personal Data Protection Act, 2023: An assessment. National Institute of Public Finance and Policy Working Paper No. 2023/04.
- PCLOB (Privacy and Civil Liberties Oversight Board). (2024). Report on the government's use of Section 702 of the Foreign Intelligence Surveillance Act (2024 review). PCLOB.
- Privacy International. (2023). State of privacy: India 2023. Privacy International.
- Rademaekers, J., Hackl, V., Leitner, C., & Siri, M. (2020). Algorithms and human rights: Study on the human rights dimensions of automated data processing techniques. Council of Europe/European Parliament Study PE 656.295.
- Ramanathan, U. (2019). Privacy is a fundamental right. Is surveillance still the norm? *Economic and Political Weekly*, 54(23), 29–37.
- Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online*, 94, 15–55.
- Rodan, G., & Hewison, K. (2014). Transparency, accountability, and authoritarianism in Southeast Asia. *Journal of Contemporary Asia*, 44(1), 1–26. <https://doi.org/10.1080/00472336.2013.822590>
- Sreevatsan, A. (2022, September 14). Inside Trinetra: Pune Police's AI surveillance system with no public documentation. *The Indian Express*.
- Srinivas, J. (2023). The Digital Personal Data Protection Act 2023: A commentary. The Vidhi Centre for Legal Policy.
- Taddeo, M., & Floridi, L. (2018). The debate on the moral responsibilities of online service providers. *Science and Engineering Ethics*, 24(6), 1575–1603. <https://doi.org/10.1007/s11948-016-9844-6>
- UIDAI (Unique Identification Authority of India). (2023). Aadhaar: Authentication transactions report 2022–23. Ministry of Electronics and Information Technology, Government of India.
- UIDAI (Unique Identification Authority of India). (2024). Aadhaar dashboard: Enrolment and authentication statistics (April 2024). Ministry of Electronics and Information Technology, Government of India. <https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india/statistics.html>
- UNESCO. (2023). Recommendation on the ethics of artificial intelligence: National implementation survey results 2022–23. United Nations Educational, Scientific and Cultural Organization.
- Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India and Others, (2017) 10 SCC 1.
- Supreme Court of India. (2018). Justice K.S. Puttaswamy (Retd.) v. Union of India and Others (Aadhaar case), (2019) 1 SCC 1.