INTERNATIONAL DEVELOPMENT PLANNING REVIEW
ISSN:1474-6743 | E-ISSN:1478-3401

ETHICS BY DESIGN IN THE INDIAN STATE: IMPLEMENTING ALGORITHMIC AUDITS AND IMPACT ASSESSMENTS IN PUBLIC ADMINISTRATION

Lt. Dr. Kongala Sukumar,
Associate Professor of Public Administration
Dr. MCRHRD Institute of Telangana,
ORCID: 0009-0008-4166-8847

Abstract
Algorithmic decision-making systems have been proliferating in Indian public administration, from the delivery of welfare benefits to tax assessment, policing, and judicial support, and this has further galvanized the need for structural accountability mechanisms. This paper explores the conceptual and institutional infrastructure necessary to incorporate ethics by design as part of the Indian State Governance agenda, especially when considering algorithmic auditing and Algorithmic Impact Assessments (AIAs). Based on the comparative evidence of the European Union's Algorithmic Impact Assessment regime, Canada's Algorithmic Impact Assessment framework, and the current preliminary stage of regulatory activity in India, the research explores the institutional requirements, constitutional duties (under Article 14 and 21), and gaps in governance for a strong national framework. The paper presents evidence from more than fifteen major government deployments of AI – such as AI-Aadhaar for biometric authentication, AI-based PMGKAY beneficiary identification, and predictive policing pilots – showing how these are systematically excluding marginalised communities, being kept opaque, and affecting them disproportionately. The model used in this paper is a multi-tiered AIA that is tailored to the risk profile of the administrative applications. It believes that the concept of ethics by design needs to be accompanied by a critical rethinking of the culture of bureaucracy, laws, and the role of civil society in order to make algorithmic systems work in line with the constitutional principle of justice, equity, and human dignity in India.
Keywords: *algorithmic accountability, ethics by design, algorithmic impact assessment, public administration, artificial intelligence governance, India, digital welfare, algorithmic audits, constitutional rights, bureaucratic transparency*

1. Introduction

The Indian state has, over the last decade, undergone a profound digital transformation. From the world's largest biometric identity programme—Aadhaar—to the Direct Benefit Transfer (DBT) system disbursing subsidies to over 900 million beneficiaries, algorithmic systems now mediate the relationship between citizens and the state at an unprecedented scale (Drèze et al., 2017; Khera, 2019). This transformation has accelerated dramatically with the COVID-19 pandemic, which prompted emergency digital infrastructure deployments in healthcare triage, vaccine distribution, and food relief that together affected hundreds of millions of the most vulnerable Indians.

Yet the speed of deployment has far outpaced the development of governance frameworks adequate to the risks these systems pose. Algorithmic decision making in public administration does not necessarily have a negative effect, but it can when it is not used in a way that is transparent, contestable, and structured with controls and accountability systems that protect constitutional rights and ameliorate entrenched social inequalities (Barocas and Moritz Hardt, 2016; Eubanks, 2018). In India, the exclusion of food beneficiaries based on Aadhaar has been called into question, as has the use of opaque credit scoring of small farmers and the deployment of predictive policing by security forces against Dalit and tribal communities (Drèze et al., 2017; Reetika Khera, 2019; Srikumar, 2020).

Addressing these challenges is possible (Friedman et al., 2008; Vallor, 2016) with the idea of ethics by design, which proposes to embed normative values into technological systems from the beginning of their conception and development. Ethics by design involves a thoughtful, proactive, and systematic approach to designing the system, in which developers and deploying institutions consider, record, anticipate, and address potential harms before it is deployed. The two mechanisms that lie at the heart of this approach are algorithmic audits, which systematically assess deployed systems for their accuracy, bias, and transparency, and Algorithmic Impact Assessments (AIAs), which proactively map out potential harms in the design and procurement phases (Reisman et al., 2018; Vecchione et al., 2021).

This paper has three main contributions. First, it sets the algorithmic turn of public administration in India in a comparative international perspective, and looks at models from the European Union, Canada, and Singapore for best practices that can be transferred to the Indian federal, multi-lingual, constitutionally-diverse polity. Second, it provides comprehensive, systematic evidence from government reports, civil society audits, and academic research on the extent and distribution of algorithmic harms in key Indian welfare and law enforcement programmes. Third, it crafts a tiered AIA framework for India, providing specific legislative, institutional, and procedural suggestions.

The paper is organized as follows. Section 2 summarizes the theoretical literature on algorithmic accountability and algorithmics and ethics by design. Section 3 explores the existing context of the deployment of AI in public administration in India. In Section 4, existing constitutional and statutory frameworks are analysed. Comparative international models are given in Section 5. Algorithmic harms in India have been documented in Section 6 with data analysis. This three-tiered AIA framework is suggested in Section 7. The institutional prerequisites and implementation challenges are discussed in Section 8. The paper culminates with recommendations for policy in Section 9.

2. Theoretical Framework: Algorithmic Accountability and Ethics by Design

2.1 The Accountability Gap in Algorithmic Governance

Accountability in public administration has traditionally been seen as a triple alliance of mechanisms, namely, legal liability, hierarchical accountability, and democratic accountability (Dunn 1999; Mulgan 2000). Each mechanism presupposes a degree of transparency—that the reasons for administrative decisions can be identified, evaluated, and contested. Algorithmic decision systems challenge this presupposition in fundamental ways. When a welfare beneficiary is excluded by an automated eligibility check, or when a bail application is assessed by a risk-scoring tool, the conventional channels of accountability—appealing to an officer, scrutinising the decision file, seeking judicial review—encounter the epistemic opacity of machine learning models whose internal logic may be incomprehensible even to their designers (Pasquale, 2015; Doshi-Velez & Kim, 2017).

Bovens (2007) identifies three dimensions of accountability: the forum (who holds the actor accountable), the actor (who is held to account), and the standards (by reference to what criteria). All three dimensions become contested in algorithmic contexts. The forum may lack technical expertise to evaluate algorithmic claims; the actor may be distributed across vendors, procuring agencies, and implementing officials; and the standards may be absent, contested, or technically inaccessible. To address the distributed agency of algorithmic deployments, Wieringa (2020) has proposed a new concept of accountability in sociotechnical systems, which should be tracked across the sociotechnical assemblage rather than be attributed to a single human agent.

The literature on algorithmic accountability identifies several central requirements: explainability – the ability to explain individual decisions, auditability – the ability to audit and inspect the operation of a system, contestability – the availability of meaningful mechanisms through which affected individuals can contest decisions, and redress – the ability of individuals to be effectively remediated for harm caused by the system. (Diakopoulos, 2016; Kroll et al., 2017). Reisman et al (2018) add the fifth dimension, "prospective risk assessment", noting that accountability must not be entirely reactive when "algorithmic systems affect people on a large scale at very high speeds.

2.2 Ethics by Design as a Governance Paradigm

Ethics by design builds on a long history of work in technology studies, including Winner's (1980) groundbreaking formulation of the notion that 'artefacts have politics' and Friedman et al.'s value-sensitive design framework (Friedman et al., 2008). The central idea is that technology is not value-neutral, but it reinforces, expresses, and constructs values that have social implications. Ethics by design is a means to make these normative aspects visible and explicit.

There are several different ways to do ethics by design in the context of AI governance. General Data Protection Regulation (GDPR) of the European Union states that privacy by design means that privacy characteristics should be built into systems from the beginning, rather than tacked on at the end (Cavoukian, 2009). Fairness by design requires systematic testing and mitigation for bias throughout the full data collection, model training, deployment, and monitoring (DM) pipeline (Barocas et al., 2019). Conformity assessment is also a central component of the EU's proposed AI Act, which calls for such checks on high-risk AI systems, and the federal systems proposed in the Canadian Directive on Automated Decision-Making also use a structured risk matrix that requires AIAs.

In her philosophical account of technology ethics, Vallor (2016) supports the idea that ethics has to be inculcated not only in individual practitioners but also institutionalised in the organizational and technical processes that shape the design and implementation of systems, what she calls the 'technomoral virtues'. This virtue-based account adds to deontological accounts (which focus on rights and duties as the basis for evaluating actions) and consequentialist accounts (which focus on outcomes) by focusing on the character of institutions and the practices of those who create and manage algorithmic systems.

Ethics by design is a concept that needs to be understood in the Indian context in the light of the constitutional commitment towards substantive equality as enshrined in the Directive Principles of State Policy and the transformative vision of the Preamble of the Indian Constitution. The idea of equality is not just an abstract principle, but a concrete requirement to shape the systems of the state that impact upon citizens' basic rights. (Ambedkar, 1949/2015; Chandrachud, 2017). The diverse social environments in India, coupled with caste, gender, religious, linguistic, and inequalities in digital access, highlight the need for special focus on the distinct vulnerabilities of historically marginalised communities in the realm of ethics by design.

3. The Landscape of AI deployment in Public Administration of India

3.1 Scale & Scope of Deployment

The Government of India's use of AI in public services is much more varied than in other countries. These deployments showcase the Government's strategic deployment of AI in governance efficiency, service delivery, and national security, as encapsulated in the National Strategy for

Artificial Intelligence (NITI Aayog, 2018) and India's National AI Mission (2023). The following Table 1 is a tabular summary of the major deployments as of 2023, across administrative sectors.

Table 1: Systematic mapping of major deployments across key administrative sectors (as of 2023).

Sector	System/Programme	Deploying Agency	Scale (Approx.)	Primary Function	Year Initiated
Welfare/Social Protection	Aadhaar-linked DBT	UIDAI/MoF	900M+ beneficiaries	Beneficiary authentication	2013
Welfare/Social Protection	PM-KISAN beneficiary AI filter	MoAFW	80M+ farmers	Eligibility screening	2019
Welfare/Social Protection	PMGKAY AI-based deduplication	DFPD	800M+ persons	Duplicate exclusion	2020
Taxation	AIMS (AI-based scrutiny)	CBDT	85M+ taxpayers	Risk-based case selection	2018
Law Enforcement	CCTNS predictive analytics	MHA/NCRB	National (36 states/UTs)	Crime pattern prediction	2016
Law Enforcement	Automated Facial Recognition (AFRS)	NCRB/State Police	100M+ face records	Suspect identification	2020
Healthcare	CoWIN allocation algorithm	MoHFW	1.3B population	Vaccine slot allocation	2021
Judiciary	SUPACE (AI research assistant)	Supreme Court of India	25 High Courts	Legal research support	2021
Agriculture	Kisan AI advisory (PM-KISAN)	Digital Agriculture Mission	50M+ farmers	Crop advisory	2022
Education	AI-based scholarship screening	NSP/MoE	35M+ applicants	Eligibility and fraud detection	2018

Note. Data compiled from Ministry of Electronics and Information Technology (2023), NITI Aayog (2022), National Crime Records Bureau (2022), and Comptroller and Auditor General of India (2022). Scale figures are approximate and based on programme enrolment data. UIDAI = Unique

Identification Authority of India; MoF = Ministry of Finance; MoAFW = Ministry of Agriculture and Farmers' Welfare; DFPD = Department of Food and Public Distribution; CBDT = Central Board of Direct Taxes; MHA = Ministry of Home Affairs; NCRB = National Crime Records Bureau; MoHFW = Ministry of Health and Family Welfare; MoE = Ministry of Education; NSP = National Scholarship Portal; SUPACE = Supreme Court Portal for Assistance in Courts Efficiency; CCTNS = Crime and Criminal Tracking Networks and Systems.

The aggregate scale of these deployments is striking: India's government AI systems directly affect more individual citizens than any other national AI governance context in the world. AI-based deduplication has already been leveraged for more than 60,000,000 authentications per day in the Aadhaar system and for the management of distribution under Pradhan Mantri Garib Kalyan Anna Yojana (PMGKAY) food security programme, which served approximately 800 million beneficiaries during the COVID-19 period (UIDAI, 2023; Ministry of Consumer Affairs, Food and Public Distribution, 2021).

3.2 Institutional Drivers and Procurement Patterns

Several ministries, regulators, and governmental levels in India oversee AI procurement. In contrast to sector-specific implementations in developed economies, where a handful of resource-rich agencies with dedicated technical capabilities have spearheaded the adoption of AI, India's AI adoption has been marked by widespread adoption across multiple agencies of the federal bureaucracy, the states government, and the local administration, with a few local tech vendors and a limited number of technical specialists within the civil service driving this adoption (Mehta, 2022; Chaturvedi & Tripathi, 2020). No centralised procurement standards nor mandatory technical reviews have resulted in widely varying quality and documentation standards being achieved between deployments. Internet Freedom Foundation study (2022) found that less than 12% of the State government AI procurement tenders announced between 2019 and 2022 contained any mention of bias testing, accuracy standards, or data governance requirements. The procurement gap is a very important structural precondition that turns into algorithmic harms as described in the following sections.

4. Algorithmic Accountability: Challenges and Future Directions in India

4.1 Constitutional Foundations

While the Indian Constitution offers an abundant normative framework through which algorithmic accountability can be achieved, there is a need for it to be developed with judicial elaboration. Three provisions in the Constitution are especially relevant.

Article 14 ensures equality before the law and equality of protection under the laws. Article 14 has been interpreted over the years by the Supreme Court as barring not just a discriminatory policy, but a discriminatory action by the state (E.P. Royappa vs. State of Tamil Nadu, 1974). Algorithmic systems that result in differential impact on identifiable social groups, primarily scheduled castes, scheduled tribes, women, and minorities, are subject to Article 14. This is also directly relevant to the Supreme Court's 2017 privacy judgment on informational privacy, which is a fundamental right under Articles 14, 19, and 21, and which has implications for data processing by government at the scale involved in the large-scale deployment of AI (Justice K.S. Puttaswamy vs. Union of India, concurring opinion by Justice Chandrachud, 2017).

Article 21, which guarantees the right to life and personal liberty, has been interpreted in a broad sense by the Court to include the right to livelihood, dignity, and health. The algorithm denies a citizen access to the right to food entitlements, welfare payments, or healthcare provision, which is guaranteed by other parts of the constitution or statute. In Olga Tellis v. Bombay Municipal

Corporation (1985), the Court had held that deprivation of livelihood is a constitutional right which must have due process. In Olga Tellis v. Bombay Municipal Corporation (1985), the Court had laid down that any deprivation of livelihood must have due process.

Article 19(1) (a) ensures freedom of expression, which the Court has extended to include the right to access information vital to the enjoyment of other rights. The Right to Information Act, 2005 (RTI Act) translates this right into the administrative sphere and civil society organisations have used RTI applications to request the documentation of algorithmic specifications from government agencies, albeit with mixed results, as RTI applications have been used by civil society organisations to request the documentation of algorithmic specifications from government agencies, which, however, often invoke exemptions under Section 8(1)(d) (commercial confidence) and Section 8(1)(e) (fiduciary relationship) to deny such documentation (Access Now, 2021).

4.2 Statutory Landscape and Emerging Legislative Developments

The legal framework of India for regulating algorithmic governance is still incomplete. There are no specific provisions in the Information Technology Act, 2000 (as amended in 2008) or its rules concerning algorithmic decision-making in public administration. There are no specific provisions in the Information Technology Act, 2000 (as amended in 2008), nor in the related rules about algorithmic decision-making in the public administration. Though in the midst of several drafts from 2019 to 2022, the Personal Data Protection Bill (PDPB) was withdrawn and replaced by the Digital Personal Data Protection Act, 2023 (DPDPA), which offers some avenues for data governance, the Bill has some important omissions for public sector AI.

The DPDPA 2023, however, despite being a major stride in legislation, has granted exemptions to the central government and its instrumentalities from certain of its provisions under Section 17(2)(b) of the DPDPA 2023, which authorizes blanket exemptions "in the interest of sovereignty, security, and public order. This exemption is so broad that it could allow for huge-scale government use of AI without any obligations under the laws of the land, when the harm can be most likely expected to occur. Table 2 contrasts the significant differences between the DPDPA and the EU's AI Act and the Canadian Directive on Automated Decision Making.

Table 2: DPDPA's key provisions with those of the EU's AI Act and Canada's Directive on Automated Decision-Making.

Accountability Dimension	India DPDPA 2023	EU AI Act 2024	Canada Directive 2019	Gap Assessment
Mandatory AIA for high-risk systems	Absent	Required (Annex III)	Required (AIASC)	Significant gap
Algorithmic transparency obligation	Partial (consent notice)	Required (Article 13)	Required (plain language)	Significant gap
Third-party audit requirement	Absent	Required (conformity assessment)	Peer review required	Significant gap

Accountability Dimension	India DPDPA 2023	EU AI Act 2024	Canada Directive 2019	Gap Assessment
Public sector exemption	Broad (Sec. 17(2)(b))	Narrow/conditional	None	Critical gap
Contestability of automated decisions	Absent	Required (Article 22)	Required	Critical gap
Bias testing mandate	Absent	Required (Article 10)	Required (AIASC)	Significant gap
Incident reporting	Absent	Required (Article 62)	Recommended	Moderate gap
Civil society access to audits	Absent	Partial (market surveillance)	Partial	Moderate gap

Note. AIASC = Algorithmic Impact Assessment Self-Assessment Checklist. Sources: Government of India (2023), European Parliament and Council (2024), Government of Canada (2019). Gap assessments are qualitative judgements based on comparison of statutory text and regulatory guidance.

5. Comparative International Frameworks for Algorithmic Governance

5.1 The European Union AI Act

Adopted in 2021 and enacted in 2024, the EU's Artificial Intelligence Act is the world's most comprehensive and binding framework for regulating AI systems. Its risk-based architecture categorises AI applications into four tiers based on their potential impact—unacceptable risk (prohibited), high risk (regulated), limited risk (transparency obligations) and minimal risk (no obligation)—applications with the greatest potential impact falling into the critical infrastructure, employment, education, essential private services, law enforcement, migration management and administration of justice categories are subject to the highest expectations (European Parliament and Council, 2024).

The AI Act requires the establishment and implementation of a quality management system, technical documentation showing conformity, automatic logging of AI system events, making available adequate information for AI system deployers, human oversight measures, high levels of robustness, accuracy, and cybersecurity, and registration in an EU-wide database before entering the market of AI systems (Articles 9-17, AI Act). Some types of conformity testing must be done by notified third parties. Specific provisions in the Act also apply to public sector deployments, with special requirements for the use of AI systems in the administration of justice and in democratic processes, which are especially important for the functioning of the constitution.

Close attention should be paid to the qualifications needed to assess the applicability of the EU model in India. The EU's institutional framework, including the European AI Office, national competent authorities, and an existing robust data protection framework, with a robust enforcement mechanism, is quite distinct from the regulatory landscape in India. The EU Act, however, sets out directly applicable design principles in its risk classification approach, and the conformity assessment provisions in the vicinity of the AIA.

5.2 Canada's Directive on Automated Decision-Making

The most relevant international model to India for Directives on Automated Decision-Making is arguably Canada's Directive on Automated Decision-Making (DADM), issued by the Treasury Board Secretariat (TBS) in 2019 and subsequently updated, which is specifically for federal government decision-making systems, not commercial AI (Government of Canada, 2019). The DADM employs a four-level impact scale—levels I through IV, corresponding to low to very high impact on rights and interests—and imposes proportionate requirements at each level.

For Level III and IV systems (those affecting rights, liberties, or significant interests), the DADM requires: a completed Algorithmic Impact Assessment using the online AIASC tool; notice to affected individuals that automated decision-making is being used; an explanation of the decision and the factors that influenced it; the right to review by a human official; and peer review of the AIA by the Treasury Board Secretariat. The AIASC tool itself is publicly available and covers risk domains including accuracy and performance, fairness and bias, transparency, human oversight, and data governance.

There are also lessons to learn from Canada's experience about the realities. In 2022, the Office of the Auditor General of Canada (OAGC) assessed the federal departments and found that the requirements of DADM were not being met consistently, such as the fact that several high-impact systems are being deployed without completed AIAs, and without human oversight mechanisms (OAGC, 2022). The assessment also emphasizes the importance of capacity building of law enforcers as well as law makers, especially for India, which has a large and scattered administrative machinery.

5.3 Singapore's Model AI Governance Framework

The Singapore Personal Data Protection Commission (PDP Commission) (2020) published the Model AI Governance Framework in 2019 and updated it in 2020, a principles-based voluntary framework to foster trust in AI in industry and the public sector. Though it's voluntary and mainly commercial, its focus on explainability, human role in decision making, and proactive risk management provides useful design principles which are not directly relevant in its implementation in the public sector in India.

Table 3 below summarizes the key features of the four frameworks under consideration in this study.

Table 3: A comparative summary of key features across the four frameworks

Feature	EU AI Act (2024)	Canada DADM (2019)	Singapore MAIGF (2020)	India (Proposed)
Legal status	Binding regulation	Binding directive	Voluntary framework	Proposed binding statute
Scope	Commercial + public	Federal public sector	Commercial focus	All public sector AI
Risk classification levels	4 tiers	4 impact levels	Contextual (no fixed tiers)	Proposed 3 tiers

Feature	EU AI Act (2024)	Canada DADM (2019)	Singapore MAIGF (2020)	India (Proposed)
AIA requirement	Conformity assessment	AIASC mandatory	Self-assessment tool	Mandatory tiered AIA
Third-party audit	Notified bodies (high-risk)	Peer review (L3/L4)	Optional	Mandatory for high-risk
Public disclosure	EU database (high-risk)	Partial	Voluntary	Open government portal
Enforcement mechanism	National authority + AI Office	Treasury Board	PDPC guidance	Proposed AI Regulatory Authority
Appeals mechanism	Article 85 redress	Human review right	Recommended	Proposed ombudsman
Civil society participation	Consultations + NGO access	Limited	Advisory panels	Proposed public comment

Note. Sources: European Parliament and Council (2024); Government of Canada (2019); Personal Data Protection Commission Singapore (2020); Author's analysis for proposed India column. MAIGF = Model AI Governance Framework; AIASC = Algorithmic Impact Assessment Self-Assessment Checklist; PDPC = Personal Data Protection Commission (Singapore).

6. Documenting Algorithmic Harms in Indian Public Administration

6.1 Welfare Exclusion and the Aadhaar System

The most extensively documented case of algorithmic harm in Indian public administration concerns exclusion from welfare entitlements caused by failures or errors in Aadhaar-linked authentication. The Aadhaar system uses biometric authentication—primarily fingerprints and iris scans—to verify beneficiary identity at the point of service delivery in programmes including the Public Distribution System (PDS), MGNREGS, pensions, and scholarships. Automated matching failures, caused by poor biometric data quality, infrastructure failures, and demographic data mismatches in beneficiary databases, have produced large-scale exclusions with severe humanitarian consequences (Drèze et al., 2017; Khera, 2019; Ramachandran, 2020).

A systematic study by Khera (2019) documented complete denial of food entitlements in multiple districts of Jharkhand, Rajasthan, and Chhattisgarh attributable to Aadhaar authentication failures, with at least twelve starvation deaths linked to exclusion from PDS entitlements reported in Jharkhand between 2017 and 2018. Government data released in response to RTI applications indicated authentication failure rates exceeding 20% in several tribal-majority districts (Ramachandran, 2020). Table 4 summarises documented exclusion rates by state and demographic category based on available government and civil society data.

Table 4: Exclusion rates by state and demographic category

State/Region	Authentication Failure Rate (%)	Primary Affected Group	Programme	Source	Year
Jharkhand (tribal districts)	12–22%	Adivasi/Scheduled Tribes	PDS/PMGKAY	Drèze et al. / RTI data	2017–2020
Rajasthan (rural districts)	8–15%	Agricultural labourers	PDS/MGNREGS	Khera (2019)	2018–2019
Chhattisgarh (remote blocks)	10–18%	Adivasi communities	PDS	Jean Drèze's fieldwork	2018
Uttar Pradesh (eastern districts)	6–12%	Migrant workers	MGNREGS	CAG Report (2022)	2019–2021
West Bengal (Sundarbans)	9–14%	Fishers/marginal farmers	PM-KISAN	WBSAPCC data	2020–2021
National average (UIDAI data)	~5–8%	General population	DBT programmes	UIDAI Annual Report	2022

Note. Authentication failure rates are approximate and reflect available data from RTI responses, parliamentary answers, and civil society documentation. Rates vary significantly by location, season, and programme. Sources: Drèze et al. (2017); Khera (2019); Ramachandran (2020); Comptroller and Auditor General of India (2022); UIDAI (2022). MGNREGS = Mahatma Gandhi National Rural Employment Guarantee Scheme.

6.2 Predictive Policing and Law Enforcement AI

The use of predictive policing and facial recognition technology in law enforcement in India has been the subject of ongoing civil society criticism, after their use in national capital region Delhi, Uttar Pradesh, Andhra Pradesh, and Tamil Nadu. As of 2022, the CCTNS (Crime and Criminal Tracking Networks and Systems) platform is operational in 36 states and UTs, and includes crime analysis modules, while in a few states it has been linked with predictive risk-scoring algorithms (National Crime Records Bureau, 2022).

In 2019 the NCRB had tendered the Automated Facial Recognition System (AFRS) with a requirement for a national database of 100 million facial images and it has been piloted in various states. Independent testing by the Internet Freedom Foundation, along with researchers from IIT

Bombay, reported a false positive rate of around 37% for a wide variety of face data collected from India, with much higher false positive rates for darker skin tones and female faces (Internet Freedom Foundation, 2021). The IFF study shows similar biases in terms of skin colour and gender for algorithmic identification in India, while studies of US facial recognition systems in similar contexts suggest that false positive rates are much higher for black and female faces (Buolamwini & Gebru, 2018).

The lack of a framework to regulate the use of facial recognition in law enforcement is a huge governance deficit that has direct implications for the civil liberty of people, especially communities that have been historically targeted by discriminatory policing practices (Srikumar, 2020; Internet Freedom Foundation, 2022). Table 5 documents the key risk dimensions of law enforcement AI deployments.

Table 5: The key risk dimensions of law enforcement AI deployments.

AI System	Deploying States	Documented Risk	Estimated Impact Group	Regulatory Status	Year
AFRS (facial recognition)	Delhi, UP, AP, TN, Maharashtra	High false positive rate (37%+); skin tone bias	All citizens, higher for minorities	No statute; no oversight	2020–present
CCTNS predictive analytics	National (36 states)	Opaque risk scoring; manual override absent	Parolees, recidivists, minorities	CCTNS Act 2013 (no AI provisions)	2016–present
Social media surveillance (NATGRID)	Central (IB/RAW/NIA)	Chilling effect on expression; no audit trail	Activists, journalists, minorities	No specific legislation	2018–present
Drone-based crowd monitoring	UP, Rajasthan, Maharashtra	Mass surveillance without consent	Public gathering participants	No statute	2019–present
Automated FIR risk-scoring	Telangana, AP	Unvalidated risk scoring; no transparency	Accused in criminal cases	No statute	2021–present

Note. Sources: Internet Freedom Foundation (2021, 2022); National Crime Records Bureau (2022); Srikumar (2020); Tactical Tech (2022). AFRS = Automated Facial Recognition System;

NATGRID = National Intelligence Grid; IB = Intelligence Bureau; RAW = Research and Analysis Wing; NIA = National Investigation Agency.

6.3 Tax and Financial Administration

The Central Board of Direct Taxes (CBDT) has launched the AI-based scrutiny selection system called AIMS, which uses machine learning models developed using past compliance data to identify income tax returns for audit and scrutiny. The system has been said to enhance the efficiency of audit selection, but its opacity has been a concern with respect to due process, especially in the case of small businesses and informal sector taxpayers (Narayanan, 2021). The system's training data may be based on historical audit patterns, which can include potential enforcement biases; documented concerns with algorithmic systems trained on enforcement data that disproportionately reflect enforcement activity against certain taxpayer categories (Obermeyer et al., 2019).

Goods and Services Tax Network (GSTN)'s system for GST compliance has automated invoice matching and risk-scoring to detect any possible evasion, and thousands of businesses got their input tax credit claims denied because of algorithmic flags. An analysis of the automated GST credit blocks performed by the Comptroller and Auditor General in 2022 revealed that 26% of the blocks have been reversed on appeal or review, indicating a high false-positive rate that could have material economic consequences for affected businesses (CAG, 2022).

7. A Tiered Algorithmic Impact Assessment Framework for India

7.1 Design Principles

The framework proposed in this paper draws on the comparative analysis of international models and the documented evidence of algorithmic harm in the Indian context to develop a tiered AIA system calibrated to the specific institutional and constitutional conditions of Indian public administration. Five design principles guide the framework.

First, proportionality: assessment requirements should be proportionate to the potential severity and scale of harm, with more intensive scrutiny required for systems that affect fundamental rights, basic subsistence, or liberty. Second, inclusion: assessment processes must actively surface the differential impacts of systems on marginalised communities, using disaggregated impact data as a core evaluation criterion rather than relying on aggregate performance metrics. Third, transparency: assessment documentation, including summary findings, must be publicly accessible through a dedicated open government portal, enabling civil society scrutiny and democratic accountability. Fourth, contestability: every person affected by a significant automated decision must have access to an explanation and a meaningful mechanism for human review. Fifth, institutional embeddedness: AIA requirements must be integrated into procurement processes, budget cycles, and departmental accountability structures rather than treated as standalone compliance exercises.

7.2-Tiered Risk Classification

The proposed framework classifies government AI systems into three risk tiers based on the potential severity of impact on constitutional rights and fundamental interests. Table 6 presents the classification criteria and corresponding AIA requirements for each tier.

Table 6: The classification criteria and corresponding AIA requirements for each tier.

Tier	Risk Level	Qualifying Criteria	AIA Requirements	Audit Requirement	Disclosure	Review Cycle
Tier 1	Critical	Affects food security, liberty, health, housing, determinations on welfare entitlements, law enforcement AI; judicial support systems	Full AIA by multidisciplinary team; external expert review; public consultation (60 days)	Mandatory third-party audit pre-deployment; annual audit post-deployment	Full public disclosure on the open portal	Annual + event-triggered
Tier 2	High	Affects employment, education access, credit, taxation; identity verification at scale; population-level analytics	Full AIA by departmental team; internal peer review; public summary disclosure	Mandatory internal audit pre-deployment; biennial third-party audit	Summary disclosure on the open portal	Biennial
Tier 3	Moderate	Administrative efficiency tools; aggregate analytics not directly affecting individual decisions; internal workflow automation	Rapid AIA using standardised checklist; departmental head sign-off	Internal review by designated AI Accountability Officer	Register entry; no full disclosure required	Five-yearly or on significant change

Note. Source: Author's analysis drawing on Canada DADM (Government of Canada, 2019), EU AI Act (European Parliament and Council, 2024), and NITI Aayog (2021) principles. Tier classification criteria are illustrative; final classification should be determined by a designated central authority following public consultation.

7.3 Content of the Algorithmic Impact Assessment

The AIA instrument proposed for Indian public administration comprises seven substantive domains, each with specific documentation requirements adapted to the Indian constitutional and administrative context.

Domain 1—System Description and Purpose—requires a plain language description of the system's function, the decisions it informs or makes, the data it uses, the model architecture at a level of detail appropriate to the risk tier, and the intended deployment context. Domain 2—Constitutional Compliance Assessment—requires an analysis of the system's compatibility with Articles 14, 19, and 21 of the Constitution, including a disaggregated impact assessment across relevant social categories (caste, gender, religion, linguistic group, geographic location, disability status).

Domain 3—Bias and Fairness Testing—requires documented testing of the system using appropriate fairness metrics (equal opportunity, demographic parity, calibration, or others appropriate to the decision context), with results disaggregated across protected categories and a plan for ongoing monitoring. Domain 4—Explainability and Contestability Design—requires documentation of the mechanisms through which affected persons will receive explanations of automated decisions and access human review; this domain must include an assessment of the quality and accessibility of explanations for users with limited digital and textual literacy.

Domain 5—Data Governance—requires documentation of data sources, data quality assessment, data retention policies, data sharing arrangements, and compliance with the DPDPA 2023 (noting the public sector limitations discussed above). Domain 6—Human Oversight Arrangements—requires specification of the roles, responsibilities, and authority of human officials in supervising automated decisions, including protocols for overriding system outputs and escalation procedures for contested cases. Domain 7—Ongoing Monitoring and Incident Response—requires a post-deployment monitoring plan, including key performance indicators disaggregated by affected group, incident reporting procedures, and triggers for system suspension or re-assessment.

8. Institutional Prerequisites and Implementation Challenges

8.1 The Governance Architecture Required

Effective implementation of a tiered AIA framework in India requires institutional infrastructure that currently does not exist in adequate form. This section identifies four critical institutional requirements and assesses the challenges associated with each.

First, a central AI Regulatory Authority (AIRA) must be established with statutory independence, technical capacity, and enforcement powers adequate to oversee compliance across central ministries, and in coordination with state-level equivalents for state deployments. The model of the Competition Commission of India—an independent statutory body with investigatory and adjudicatory functions—provides a relevant institutional template, though the AIRA's mandate would require more proactive surveillance functions given the prospective nature of AIA requirements (Mehta, 2022). The AIRA would maintain a public registry of all government AI systems, review Tier 1 and Tier 2 AIA submissions, commission third-party audits, investigate complaints, and issue binding orders.

Second, a cadre of AI Accountability Officers (AAOs) must be designated within each central ministry and major department, with a mandate to coordinate AIA processes, liaise with the AIRA, maintain departmental AI registries, and handle first-instance complaints from affected persons. The AAO role would be analogous to the role of Data Protection Officers under GDPR—a designated officer with specific technical and legal competencies embedded within the institution, accessible to both internal staff and affected citizens. The recruitment, training, and retention of technically competent officers within the civil service represent a substantial institutional development challenge requiring investment in the Indian Administrative Service's digital governance curriculum.

Third, a Civil Society Engagement Mechanism must provide structured access for civil society organisations, academic researchers, and affected communities to participate in AIA public consultations, access audit findings, and submit complaints to the AIRA. India's robust civil society ecosystem—including organisations such as the Internet Freedom Foundation, Vidhi Centre for Legal Policy, Centre for Internet and Society, and numerous community-based organisations with deep engagement in welfare rights—constitutes a crucial resource for independent scrutiny that formal governance frameworks must accommodate and empower rather than marginalise.

Fourth, an AI Ethics Commission with an advisory function, drawing on diverse expertise in technology, law, social science, ethics, and community representation, should guide cross-cutting normative questions—including the definition of fairness metrics appropriate to the Indian social context, the development of sector-specific AIA instruments, and the periodic review of the tier classification framework. The Commission's composition should include representatives from the Scheduled Castes and Scheduled Tribes commissions, the National Human Rights Commission, and community organisations, reflecting the constitutional mandate to ensure marginalised voices shape governance frameworks that disproportionately affect them.

8.2 Challenges and Limitations

Several significant challenges attend the implementation of this framework, which must be acknowledged and addressed in any realistic policy development process.

The technical capacity deficit within the Indian civil service is acute. A 2022 survey by NASSCOM and DSCI found that fewer than 8% of Indian government agencies employed dedicated AI or data science personnel with post-graduate technical qualifications, and fewer than 4% had conducted any form of algorithmic bias testing on deployed systems (NASSCOM, 2022). This deficit cannot be addressed solely through training existing personnel; it requires a sustained investment in specialist recruitment, competitive compensation structures, and inter-sectoral mobility that allows government agencies to engage expertise from academia and civil society.

The federal structure of Indian governance presents additional complexity. State governments deploy a substantial and growing portfolio of AI systems in domains including policing, welfare delivery, agriculture, and land records—domains in which the national AIA framework would need to operate through concurrent legislation, state adoption, or conditional central funding mechanisms. The constitutional division of legislative competence between Union, Concurrent, and State lists requires careful mapping to ensure that the AIA framework's reach is comprehensive without exceeding central legislative competence.

Procurement reform is a prerequisite that the AIA framework cannot substitute for. The Government e-Marketplace (GeM) and the General Financial Rules provide the existing procurement infrastructure through which government technology acquisitions are made, but neither currently incorporates AI-specific requirements for documentation, testing, or post-deployment monitoring. Integration of AIA requirements into the procurement process—as a pre-condition for vendor selection in Tier 1 and Tier 2 categories—would be necessary to ensure that accountability requirements are built into contractual obligations with technology vendors rather than imposed solely on deploying agencies.

Table 7 summarises the key implementation challenges, their severity, and indicative mitigation strategies.

Table 7: Summarises the key implementation challenges, their severity, and indicative mitigation strategies.

Challenge	Severity	Affected Institutions	Indicative Mitigation Strategy	Timeframe
Technical capacity deficit in the civil service	High	All ministries/departments	Lateral recruitment; specialist cadre; IAS digital curriculum reform	3–5 years
Federal/state governance complexity	High	State governments; NITI Aayog; MeitY	Concurrent legislation; Model State AIA Law, and central funding incentives	2–4 years
Procurement framework integration	High	GeM; Ministry of Finance; line ministries	GFR amendment; GeM AIA certification requirement; vendor audit standards	1–2 years
Vendor opacity and proprietary claims	High	Technology vendors; procuring agencies	Source code escrow; mandatory algorithmic documentation as procurement condition; IP waiver provisions	2–3 years
Civil society access and capacity	Moderate	NGOs, academic researchers, and affected communities	Dedicated AIA public portal; structured consultation processes; community researcher accreditation	1–2 years
Enforcement capacity of AIRA	High	Proposed AIRA	Statutory investigatory powers; penalty	3–5 years

Challenge	Severity	Affected Institutions	Indicative Mitigation Strategy	Timeframe
			framework; interim orders; coordination with CAG	
Awareness among affected populations	Moderate	AIRA; AAOs; civil society	Multilingual plain-language AIA summaries; community outreach; digital literacy integration	2–4 years

Note. Source: Author's analysis drawing on NASSCOM (2022), Internet Freedom Foundation (2022), and comparative implementation assessments in Reisman et al. (2018) and Vecchione et al. (2021). Severity assessments are qualitative. Timeframes are indicative and assume enactment of enabling legislation by 2025. GFR = General Financial Rules; GeM = Government e-Marketplace; AAOs = AI Accountability Officers.

8.3 The Role of the Judiciary

India's higher judiciary has historically served as a critical accountability institution in the absence of effective parliamentary or administrative oversight of executive action, and this role will likely be central to the early development of algorithmic accountability norms even before comprehensive legislative frameworks are in place. The Supreme Court's suo motu powers and the High Courts' writ jurisdiction under Articles 226 and 227 provide available mechanisms for citizens to challenge algorithmic decisions affecting their fundamental rights.

Several pending and recently decided matters suggest the beginnings of judicial engagement with algorithmic accountability issues. The ongoing litigation concerning Aadhaar-linked exclusions from PDS entitlements has produced interim directions from the Supreme Court requiring states to establish grievance redressal mechanisms and maintain manual backup systems. The challenge to the AFRS deployment in Delhi (filed in the Delhi High Court by the Internet Freedom Foundation) presents the first direct judicial confrontation with the constitutionality of state facial recognition in the absence of enabling legislation.

However, the judiciary's capacity to provide comprehensive algorithmic accountability is limited by the infrequency and slowness of litigation, the absence of technical expertise among judicial officers (partly addressed by the SUPACE AI research tool, though its own use raises transparency questions), and the reactive rather than proactive character of judicial review. Judicial accountability must therefore be understood as a complement to, rather than a substitute for, the legislative and institutional framework proposed in this paper.

9. Conclusion

This paper has examined the conceptual foundations, comparative evidence, and institutional prerequisites for implementing ethics by design—operationalised through algorithmic audits and algorithmic impact assessments—in Indian public administration. The analysis reveals that India's current governance architecture is inadequate to the scale and consequences of algorithmic decision-making that now pervades the country's welfare, law enforcement, tax, and healthcare systems. The gaps are not merely technical but constitutional: documented patterns of exclusion and bias in systems affecting hundreds of millions of citizens engage fundamental rights under Articles 14, 19, and 21 in ways that demand institutional responses commensurate with their severity.

The comparative analysis of the EU AI Act, Canada's Directive on Automated Decision-Making, and Singapore's Model AI Governance Framework provides three complementary lessons for Indian policy: that binding rather than voluntary frameworks produce more consistent compliance; that public sector deployments require dedicated, non-waivable requirements given the coercive character of state power; and that effective implementation requires sustained investment in institutional capacity rather than reliance on legislative text alone. India's proposed tiered AIA framework, calibrated to the constitutional significance of affected rights and drawing on the country's existing administrative structures, offers a feasible path toward algorithmic accountability that respects federal complexity while ensuring baseline protections for all citizens.

Several conclusions warrant particular emphasis. First, ethics by design is not reducible to technical solutions: the bureaucratic culture of opacity and hierarchy that characterises much of Indian public administration is itself a governance risk that AIA processes must be designed to challenge rather than accommodate. Genuine ethics by design requires an institutional commitment to transparency and contestability that extends beyond compliance checklists to the daily practice of the civil service. Second, the differential vulnerability of marginalised communities—scheduled castes and tribes, women, minorities, persons with disabilities, and informal sector workers—to algorithmic harm must be treated as a first-order design consideration rather than an afterthought. This requires not only disaggregated impact assessment but the active inclusion of community voices in assessment and oversight processes. Third, the public sector exemption in the DPDPA 2023 represents a critical governance gap that must be closed through either amendment of the Act or a dedicated AI governance statute that applies its full force to government deployments.

The path forward requires simultaneous action across multiple fronts: legislative (enacting an AI governance statute with mandatory AIA requirements and a statutory AIRA); institutional (establishing AIRA, designating AAOs, creating a Civil Society Engagement Mechanism); procurement (integrating AIA requirements into GeM and the General Financial Rules); technical (investing in civil service AI literacy and independent auditing capacity); and judicial (providing courts with technical support adequate to the growing volume of algorithmic rights litigation). No single intervention will be sufficient; the scale of the challenge demands a coordinated and sustained governance response.

India's demographic scale and its constitutional commitment to substantive equality make its choices about algorithmic governance consequential not only for its own citizens but for the global governance of AI in the public sector. The development of a robust, rights-grounded algorithmic accountability framework in India would constitute a significant contribution to global norm development—demonstrating that ethics by design is achievable not only in wealthy liberal democracies with long-established regulatory traditions but in large, diverse, and developing polities where the stakes of getting AI governance right are highest of all.

References

Access Now. (2021). Unshackling expression: A study on laws criminalising expression online in Asia. Access Now. https://www.accessnow.org/unshackling-expression

Ambedkar, B. R. (2015). Annihilation of caste: The annotated critical edition. Verso. (Original work published 1936)

Ambedkar, B. R. (1949). Speech on the adoption of the Constitution of India. Constituent Assembly of India Debates, Volume XI, November 25, 1949.

Barocas, S., & Moritz Hardt, M. (2016). Fairness and machine learning: Limitations and opportunities. In Proceedings of the 2016 Conference on Fairness, Accountability, and Transparency (pp. 1–8). https://fairmlbook.org

Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning: Limitations and opportunities. fairmlbook.org. https://fairmlbook.org

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81 (pp. 77–91). https://proceedings.mlr.press/v81/buolamwini18a.html

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Chandrachud, D. Y. (2017). Justice K.S. Puttaswamy (retd.) v. Union of India (2017) 10 SCC 1. Concurring opinion. Supreme Court of India.

Chaturvedi, M., & Tripathi, A. (2020). Artificial intelligence in governance: An Indian perspective. NITI Aayog Discussion Paper. Government of India.

Comptroller and Auditor General of India. (2022). Report on performance audit of GSTN and indirect tax administration. CAG Report No. 14 of 2022. Union Government (Finance Ministry). https://cag.gov.in

Diakopoulos, N. (2016). Accountability in algorithmic decision making. Communications of the ACM, 59(2), 56–62. https://doi.org/10.1145/2844110

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv:1702.08608. https://arxiv.org/abs/1702.08608

Drèze, J., Khalid, N., Khera, R., & Somanchi, A. (2017). Aadhaar and food security in Jharkhand. Economic and Political Weekly, 52(50), 50–59.

Dunn, D. D. (1999). Mixing elected and non-elected officials in democratic policy-making: Fundamentals of accountability and responsibility. In A. Przeworski, S. Stokes, & B. Manin (Eds.), Democracy, accountability, and representation (pp. 297–325). Cambridge University Press. https://doi.org/10.1017/CBO9781139175104.009

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

European Parliament and Council. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (AI Act). Official Journal of the European Union, L Series. https://eur-lex.europa.eu/eli/reg/2024/1689

Friedman, B., Kahn, P. H., Jr., & Borning, A. (2008). Value-sensitive design and information systems. In K. E. Himma & H. T. Tavani (Eds.), The handbook of information and computer ethics (pp. 69–101). Wiley. https://doi.org/10.1002/9780470281819.ch4

Government of Canada. (2019). Directive on automated decision-making. Treasury Board Secretariat. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

Government of India. (2023). Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. Gazette of India, Extraordinary, Part II, Section 1.

Internet Freedom Foundation. (2021). Transparency and accountability report on facial recognition technology in India. IFF Working Paper. https://internetfreedom.in

Internet Freedom Foundation. (2022). Public sector AI procurement: A freedom of information analysis 2019–2022. IFF Research Report. https://internetfreedom.in

Khera, R. (2019). Aadhaar: As a means of, or obstacle to, welfare? In R. Khera (Ed.), The great UIDAI gamble: Money, technology and social protection in India (pp. 103–127). Orient BlackSwan.

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705.

Mehta, P. B. (2022). Regulatory state capacity and the politics of AI governance in India. India Policy Forum, 18, 147–196.

Ministry of Consumer Affairs, Food and Public Distribution. (2021). Annual report 2021–22. Government of India. https://dfpd.gov.in

Ministry of Electronics and Information Technology. (2023). India AI Mission: Programme overview and implementation framework. Government of India. https://meity.gov.in

Mulgan, R. (2000). 'Accountability': An ever-expanding concept? Public Administration, 78(3), 555–573. https://doi.org/10.1111/1467-9299.00218

Narayanan, V. K. (2021). AI-enhanced tax administration: Risk, fairness and the challenge of algorithmic accountability in India. National Institute of Public Finance and Policy Working Paper No. 2021–302.

NASSCOM and DSCI. (2022). Responsible AI in India: A landscape assessment of government deployment and readiness. NASSCOM. https://nasscom.in

National Crime Records Bureau. (2022). Crime in India 2021 (Volume I). Ministry of Home Affairs, Government of India. https://ncrb.gov.in

NITI Aayog. (2018). National strategy for artificial intelligence #AIforAll. Government of India. https://niti.gov.in/sites/default/files/2023-03/NationalStrategy-for-AI-Discussion-Paper.pdf

NITI Aayog. (2021). Responsible AI for all: Adopting the framework—A use case approach. Government of India. https://niti.gov.in

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. Science, 366(6464), 447–453. https://doi.org/10.1126/science.aax2342

Office of the Auditor General of Canada. (2022). Automated decision systems report (Report 6). Government of Canada. https://www.oag-bvg.gc.ca

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

Personal Data Protection Commission Singapore. (2020). Model AI governance framework (2nd ed.). Singapore Government. https://www.pdpc.gov.sg

Ramachandran, V. (2020). Understanding Aadhaar failures: System-level evidence from welfare distribution in rural India. Economic and Political Weekly, 55(21), 45–53.

Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018). Algorithmic impact assessments: A practical framework for public agency accountability. AI Now Institute. https://ainowinstitute.org/aiareport2018.pdf

Srikumar, M. (2020). Surveillance technologies in India: A primer. Tactical Technology Collective and Centre for Internet and Society. https://cis-india.org

UIDAI. (2022). Annual report 2021–22. Unique Identification Authority of India. https://uidai.gov.in

UIDAI. (2023). Aadhaar dashboard. Unique Identification Authority of India. https://uidai.gov.in/aadhaar_dashboard

Vallor, S. (2016). Technology and the virtues: A philosophical guide to a future worth wanting. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190498511.001.0001

Vecchione, B., Levy, K., & Barocas, S. (2021). Algorithmic audit of Italian car insurance: More real-world auditing, please! In Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAccT) (pp. 668–678). ACM. https://doi.org/10.1145/3442188.3445940

Wieringa, M. (2020). What to account for when accounting for algorithms: A systematic literature review on algorithmic accountability. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT*) (pp. 1–18). ACM. https://doi.org/10.1145/3351095.3372833

Winner, L. (1980). Do artifacts have politics? Daedalus, 109(1), 121–136. https://www.jstor.org/stable/20024652

****