I. The Legal, Institutional, &Technical Architecture of ADMS in India

Section 1:
The Legal, Institutional and Technical Architecture of ADMS in India

AI Observatory

This project was undertaken as a part of Divij Joshi's project as a Mozilla Fellow, and is supported by Mozilla.

Designed and typset by Design Beku

Laws, Policies, Actors and Institutions

To understand the consequences of the use of ADMS and AI, it is imperative to explore the political, legal and institutional context within which its development and deployment is taking place. This section marks out the legal and institutional frameworks within which AI and ADMS are being adopted in India, and the policies and actors which are shaping the manner in which it is developed and deployed.

The Politics of AI Policy in India

The use of 'AI'-based computer systems in supporting government administration and decision-making in India can be traced back to at-least the 1980's, with the establishment of research centres for AI, like the Centre for the Development of Advanced Computing, or 'nodal centres' within the Department of Electronics which developing AI systems for government administration, supported by international development organisations like the UNDP.[1]

Early examples of ADMS in India include systems like Eklavya, a software system which aided frontline child health workers with making decisions about diagnosis, health risk and future action for healthcare.[2] Similarly, there is documented use of 'Automated Legal Reasoning Systems' under the Knowledge Based Computer Systems programme of the Government of India.[3] These systems implemented rule-based and logic-based programmes for decision making, which were piloted in the fields of income tax, pension and customs. These systems attempted to encode the logic of statutory rules in these fields into programmatic computer languages in order to aid bureaucrats in complex legal and administrative problems. These early examples are indicative of the Government of India's desire to embed ADMS within government administration to ensure consistency in decision-making, and to assist administrative agencies in navigating and administering complex rule-based systems.

The contemporary use of ADMS in India is also justified based on their efficiency in solving complex problems in government administration. However, today, ADMS adoption is occurring in a very different technological and political context, and this transformation is critical in understanding the role that ADMS plays in public agencies in India today.

Developing 'AI' and promoting computational data analytics within the government and the private sector alike has recently become a policy priority for the Government of India, as well as various state governments, over the last few years. Various 'AI' policies have been released by the Government of India – from

[1] Saint-Dizier P, 'The Knowledge-Based Computer System Development Program of India: A Review' (1991) 12 AI Magazine 33

[2] Chandrasekhara MK, Shanthi B and Mahabala HN, 'Can Community Health Workers Screen under 5yr Children with Computer Program' (1994) 61 The Indian Journal of Pediatrics 567

[3] Bajaj KK, Dubash RK and Kowalski R, 'Central Government Pension Rules as a Logic Program' in S Ramani, R Chandrasekar and KSR Anjaneyulu (eds), Knowledge Based Computer Systems, vol 444 (Springer-Verlag 1990) <http://link.springer.com/10.1007/BFb0018365>

the government policy agency NITI Aayog's National Strategy for AI,[4] to reports of expert committees constituted by the Ministry of Electronics and IT[5] – which see AI as a transformational technology, and as a crucial 'factor of production' for obtaining higher economic growth in the information economy. These policy documents have called for greater development and adoption of 'AI' across the private and public sectors, ranging from healthcare to agriculture. According to some policy documents, 'AI' is expected to operate as the infrastructure through which a number of applications and information-based tools can be built and used. For example, the Department of Telecommunications has articulated a vision for an 'AI Stack' – a technological architecture for AI as infrastructure to be developed and used across a number of applications and domains.[6]

AI development has also been a policy agenda for state and local governments. Telangana, for example, has reflected its proposals to promote and utilise ADMS and AI systems across different industries and uses, in the '2020 Year of AI Vision'.[7] Other documents like 'Tamil Nadu Safe and Ethical AI Policy' also indicate a growing recognition of the need to contend with emerging ethical issues arising from the use of AI, including fairness, transparency and accountability.[8]

> ***The vision of 'AI' articulated in these documents is one of a 'public good', championed by private firms and companies developing these technologies, and incentivised and legitimised through government policy, investment,and 'public-private partnerships'.***

This vision of AI has also influenced key regulatory and policy developments in India, particularly regarding the governance of digital data. Government policy documents, such as Economic Survey of India of 2018-2019, the Draft E-Commerce Policy[9] and the Report of the Committee of Experts on Non-Personal Data,[10] have attempted to reclassify 'data' within digital environments as an economic asset, whose value can be 'unlocked' or exploited through appropriately channeling them within AI or data analytics systems.

[4] 'National Strategy on Artificial Intelligence,' NITI Aayog, <https://niti.gov.in/national-strategy-artificial-intelligence>

[5] 'Artificial Intelligence Committees Reports', Ministry of Electronics and Information Technology, Government of India, (2020) <https://www.meity.gov.in/artificial-intelligence-committees-reports>

[6] 'Indian Artificial Intelligence Stack - Discussion Paper', Department of Telecommunications, Government of India (2020) <https://www.tec.gov.in/pdf/Whatsnew/ARTIFICIAL%20INTELLIGENCE%20-%20INDIAN%20STACK.pdf>

[7] '2020 Is Telangana's Year of AI', Information Technology, Electronics & Communications Department, Government of Telangana, <https://it.telangana.gov.in/2020-is-telanganas-year-of-ai/>

[8] 'Safe and Ethical AI Policy', Government of Tamil Nadu, (2020) <https://tnega.tn.gov.in/assets/images/pdf/AIPolicy2020.pdf>

[9] 'Draft E-Commerce Policy', Ministry of Commerce, <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1575760>

[10] Report of the Committee of Experts on Non-Personal Data Governance Framework', (2020) <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>

The policy focus on spurring innovation through the deployment of government regulation has had a direct influence on legislative policy as well. The Personal Data Protection Bill, in 2019, had carved out specific exemptions for activities like Credit Scoring and Fraud Detection, which are common use cases for ADMS.[11] Similarly, the PDP Bill also allowed for the acquisition of any 'non-personal' data by the Government, for 'better targeting' of services or for the formulation of 'evidence-based policy' – once again evidencing attempts to use 'big data analytics' within ADMS to make consequential policy and administrative decisions.[12]

While there has been an increasing recognition of the risks posed by delegating decision-making to automated systems and 'AI', particularly on risks to data protection and privacy, policy documents have understood these are primarily risks caused by technological failure, which can be allayed by appropriate technical standards (such as anonymisation of data, or through 'consent management systems').

However, even as 'AI' policy which emerges from India recognises some risks and harms in the development and deployment of AI,[13] there is a disturbing lack of recognition or regulation around the systems currently in use and being deployed. As documented in this toolkit, many decisions consequential to individuals and communities are being delegated to algorithmic systems, varying in sophistication, but posing concerns – of democratic control, justice and self-determination – which are not reflected within policies which encourage the development and deployment of 'AI' systems. In fact, even the documented deployment of current AI and Machine Learning systems does not reflect the concerns of data protection or 'ethical design' which are envisaged in policy documents at the ministerial level, pointing to the complete absence of a structural framework to ensure accountability of ADMS on the ground, even as their harms are being recognised in policy. Instead, the development of these systems is taking place in a regulatory vacuum, resulting in a situation where important considerations of transparency, accountability and democratic control are not given their due regard.[14]

Taking the gaze away from high-level policy documents on AI released by government agencies, the development of ADMS in India is being shaped, in fact, by a network of public and private actors, norms and institutions, seemingly unguided by the visions of 'ethics' or 'social good' articulated in policy documents. The case studies below shine a light on actors and institutions responsible for developing and deploying ADMS in India.

[11] Section 14, Personal Data Protection Bill, 2019. (Bill No. 373/2019)

[12] Section 91(2), Personal Data Protection Bill, 2019. (Bill No. 373/2019)

[13] See, for example, 'Working Document: Enforcement Mechanisms for Responsible #AIforAll', NITI Ayog, (2020) <https://niti.gov.in/sites/default/files/2020-11/Towards-Responsible-AI-Enforcement-of-Principles.pdf>

[14] Basu, A., Hickok, E., 'Artificial Intelligence in the Governance Sector in India', The Centre for Internet and Society, India, <https://cis-india.org/internet-governance/ai-and-governance-case-study-pdf>

[Case Study: ADMS in Policing]

Since 2016, the Federation of the Indian Chambers of Commerce and Industry (FICCI), a major industry association in India, has been instituting the 'Smart Policing Awards',[15] ostensibly with the intention of promoting practices for the safety and security of Indians. The awardees over the last four years have included Automated Decision Making Systems like the Punjab Artificial Intelligence System (PAIS), Trinetra in Uttar Pradesh, and Automated Facial Recognition and Number-Plate Recognition Systems in Madhya Pradesh, among others.

Looking over the awardees of 'Smart Policing' gives a good indication of the directions in which technology use in policing is heading, and the actors driving this change. Since the Crime and Criminal Tracking Network System (CCTNS) was first projected as the digital infrastructure to enable 'smarter' policing in India, there has been a proliferation of data-driven and digital surveillance-based technologies among policing agencies. Government agencies are funnelling substantial resources into the procurement of sophisticated surveillance and crime analytics systems, including social media and internet communications surveillance systems, as well as video surveillance and data analytics systems to be utilised in public spaces including railways and airports, as well as across public spaces in cities.

ADMS is transforming the face of law enforcement and the criminal justice system. Historical police practices, encoded in the often archaic frameworks in policing regulation like the police manuals or the police acts – are being supplemented or supplanted by 'data-driven' decisions through the use of algorithmic systems. These systems are being used to determine who gets policed – evidenced through so-called 'predictive policing' systems like the CMAPS used by the Delhi Police to indicate 'criminal hotspots', or the 'sentiment analysis' software used by Mumbai and Uttar Pradesh Police, which scans social media to 'alert' police forces of potential areas of disturbance.

ADMS is also being used to expand the reach of policing beyond the restrictions imposed by the beat of a constable or the traditional jurisdiction of a police station. ADMS is moving policing from targeted, suspicion-driven policing and surveillance, which is triggered by police procedure and legal rules, to programmatic and ubiquitous surveillance triggered by algorithmic thresholds and logics.[16]

ADMS is transforming the role and function of policing institutions in India, and not always in a positive way. When automated systems make decisions about whom to surveil, police and investigate, it can embroil individuals within a web of surveillance and incarceration, and, in particular, can reinforce systematic failures within a policing system in dire need of reform including systematic discrimination towards marginalised populations.

[15] 'Compendium of Best Practices in Smart Policing', FICCI, (2019) <http://ficci.in/spdocument/23116/FICCI-Compendium-of-Best-Practices-in-sMART-Policing-2019.pdf>

[16] Brayne S, 'Big Data Surveillance: The Case of Policing' (2017) 82 American Sociological Review 977

There is very little empirical evidence of how ADMS is impacting law enforcement in India.[17] While private companies and bureaucrats tout the effectiveness and accuracy of these systems, the automated turn in policing has not been scrutinised for its reliability, nor has there been any systematic effort at understanding ADMS use in policing and its impact on civil liberties or community harms. There has also been no systematic attempt at revising police practice or procedure – from policing manuals to forensic practice – to contend with or govern the use of ADMS.

> ***How can we ensure that ADMS in policing and criminal justice institutions is not used for unjust surveillance and punishment?***

[17] There are progressive efforts to study the use of ADMS in policing, see, for example, Narayan, S, and Marda, V, 'Data in New Delhi's Predictive Policing System, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, <https://dl.acm.org/doi/abs/10.1145/3351095.3372865>, 'Project Panoptic', Internet Freedom Foundation, <https://internet-freedom.in/tag/project-panoptic>; Mathews H V, Sinha A., 'Use of Algorithmic Techniques for Law Enforcement', 55(23) Economic and Political Weekly (2020).

[Case Study: ADMS in Smart Cities]

In June, 2015, the Government of India launched the Smart Cities Mission, a project which envisages networked digital technologies at the heart of managing urban spaces and livelihoods. India's Smart City project aims to create massive, city-wide digital infrastructure which can solve mundane and persistent issues of urban governance – providing basic utilities, ensuring citizen safety, and making cities 'future proof'. ADMS are now routinely embedded in public infrastructure, responsible for decisions about our lives and livelihoods – from safety and sanitation, to the supply of basic utilities like electricity and water.[18]

Smart City projects are important institutional forces behind the proliferation of ADMS in India. The models of urban governance in the Smart City are quite explicit in their attempts at governance through surveillance and datafication, both of urban environments and residents.[19] Integrated Command and Control Centres, connected by city-wide Closed Circuit TV's, use 'intelligent' algorithmic machine vision tools to identify and alert officials of 'loitering' citizens, or allow city police to predict possible violent crimes.[20] In the 'smart cities' of Chandigarh, Nagpur and Indore, workers who maintain urban infrastructure are fitted with 'Human Efficiency Trackers' which automatically deduct pay if they depart from the work schedules or routes determined by algorithmic systems, not only normalising invasive surveillance of individuals, but also undermining worker agency and channels of negotiation and grievance redress.

ADMS in Smart Cities are also used to make decisions about the design of urban infrastructures, which are based on digital inputs gathered, for example, from sensored utility networks, or road transportation systems. In Bengaluru, IBM's 'smart water' solutions have attempted to use Big Data analytics to make decisions about water supply infrastructure.[21] Intelligent Traffic Management Systems are used in conjunction with cameras and environmental sensors to determine traffic in cities like Chennai, Bengaluru and New Delhi, and to assist in planning for transport and mobility infrastructure.

Smart Cities in India are being enabled through the privatisation of urban infrastructure and a departure from democratic participation and modes of governance. 'Public Private Partnerships' abound, and the city governance is corporatised as a 'Special Purpose Vehicle' – not quite state, neither entirely corporate – ostensibly to remove messy obstacles towards urban development, but in the process privatising essential utilities and shielding actors and institutions from accountability for digital infrastructure.

The institution of the Smart City may be leading us towards privatised, opaque and exclusionary digital infrastructures, and routine surveillance of urban residents.

> ***How do citizens participate in and demand accountability for automated decision-making in our 'Smart Cities'?***

[18] A snapshot of projects relevant to ADMS in Smart Cities can be seen here - http://smartcities.gov.in/content/innerpage/smart-solutions.php.

[19] Kitchin R, 'The Ethics of Smart Cities and Urban Science' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160115

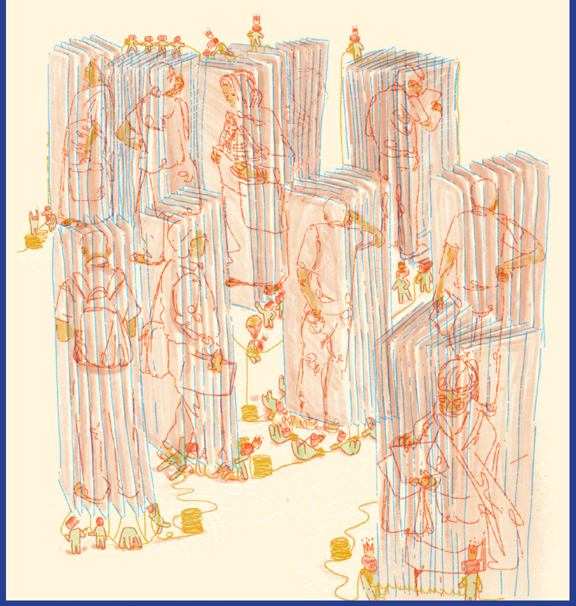
[20] See, for example, the 'Model RFP For Implementation of Smart City Solutions', https://smartnet.niua.org/sites/default/files/resources/vol_2_first_draft_rfp_for_system_integrator_scope_of_work_0.pdf

[21] Taylor L and Richter C, 'The Power of Smart Solutions: Knowledge, Citizenship, and the Datafication of Bangalore's Water Supply' (2017) 18 Television & New Media 721

[Case Study: ADMS in Welfare Administration]

In 2018, the Supreme Court of India upheld the constitutionality of the Government of India's Unique Identification Project, or Aadhaar.[22] In responding to the argument that the biometric technologies used to authenticate individual claims to welfare entitlements were based on probabilistic techniques, and were inherently exclusionary, the Court held that a technology which afforded access to social welfare could not be invalidated on the grounds of 'exclusion of a few'.

Aadhaar laid the foundation for a proliferation of ADMS and algorithmic tools within government welfare schemes – from determining eligibility for housing, to identification for ration and utility subsidies, to determining welfare fraud in government-sponsored credit programmes. As noted by the UN Special Rapporteur on Extreme Poverty, these systems are leading us to a 'digital welfare dystopia' - a rights-free zone with no protections or accountability to preserve institutions and ideals of social security.[23]


Unique Identification Project

The algorithmic turn towards the digital welfare state is apparent from programmes like the Government of Telangana's Samagra Vedika, which uses machine learning to make decisions about eligibility for housing and pension schemes, or the Government of Orissa's Kalia scheme, in which a private company provided 'big data analytics' solutions to purge the Government's list of welfare beneficiaries, only to be faced with substantial backlash from legitimatbeneficiaries.[24]

ADMS systems offer the possibility of efficiency and neutrality in welfare administration, which is a major attraction for resource-starved bureaucracies tasked with a range of administrative functions. However, these systems are being deployed without any critical interrogation regarding their limitations and their consequences. Systems of 'fraud detection' and beneficiary eligibility are utilising obscure and uncertain metrics under the guise of 'AI' and Big Data to make judgements about individual identities and claims, and ultimately, these technologies may become a barrier to entitlements, instead of a means to access welfare.

> ***How do we challenge ADMS that are used to dispossess people of their rights and entitlements?***

[22] Justice K.S. Puttaswamy v Union of India (2019) 1 SCC 1

[23] UNGA, 'Report Of The Special Rapporteur On Extreme Poverty And Human Rights', A/74/493, (October 11 2019).

[24] 'Number of Ineligible KALIA Beneficiaries Is Only 32000, Not 3.41 Lakh: Minister' (The New Indian Express) <https://www.newindianexpress.com/states/odisha/2019/sep/19/number-of-ineligible-kalia-beneficiaries-is-only-32000-not-341-lakh-minister-2035722.html>

The Regulatory Landscape of ADMS in India

There is no statute or legislative framework which explicitly attempts to regulate ADMS, algorithms, or Artificial Intelligence in India across contexts. However, ADMS regulation can be examined from how the law interfaces with its different components – namely, data and databases, algorithms and computer programmes, and within its sectoral and context-specific applications.

Regulation of Data and Databases

One legal framework which is pertinent to ADMS is that around privacy and the protection of personal data – particularly since many consequential ADMS are reliant upon the algorithmic processing of personal information. In India, Section 43A of the Information Technology Act, 2000, attempts to regulate the use of data by private entities, and the Sensitive Data and Personal Information Rules, 2011.[25] However, this legal framework does not apply to public agencies and government establishments, and has significant limitations in terms of its scope, the agency it provides to individuals to control personal data, as well as the structural mechanisms it establishes for data protection. While a more comprehensive 'Personal Data Protection Bill, 2019' has been deliberated by the Government of India, as at the time of writing, it has not been enacted.

The Supreme Court of India has articulated a fundamental Right to Privacy under the Constitution of India, which explicitly includes the right to informational privacy, self-determination over personal data, as well as agency over intimate decisions.[26] While there has been no explicit application of the Right to Privacy to automated data processing within ADMS or AI, it is a touchstone to assess and challenge harmful systems.

Regulation of Algorithms and Data Processing

ADMS deployed within specific projects or systems are occasionally the subject of specific regulations. For example, the Aadhaar Act, 2016,[27] attempts to regulate the functioning of the Government of India's Unique Identification project by specifying the standards of softwares and other technologies to be used within the ADMS systems deployed by Aadhaar, such as biometric authentication systems. Similarly, the Security and Exchange Board of India (SEBI) has auditing requirements for financial actors utilising AI or ML systems.[28]

However, there are no regulations specific to algorithmic systems within government systems or other consequential decision-making systems, which specify standards or structures for ensuring transparency and accountability for certain broad classes of algorithmic systems (as, for example, under the French Digital Republic Act).[29] Similarly, there are no norms around how to audit or investigate algorithmic systems used within public or private agencies, which is a necessary starting point for determining whether a system is functioning as it should, and what kinds of assumptions or biases an algorithmic system may embody.

Legal systems around the world are increasingly recognising algorithmic systems as sites of regulation, to ensure that they abide by important rights and values within those jurisdictions. For example, the General Data Protection Regulation (GDPR) in the European Union recognises the need to provide protections against decisions made by automated systems which have legal consequences, including the right to have human involvement in such decisions, as well as to demand explanations for such decisions.[30] Similarly, governments are mooting approaches towards structural regulation of consequential algorithmic systems. The Algorithmic Accountability Act introduced in the USA, for example, attempts to regulate the use of certain algorithmic systems through mandatory reporting, audits and impact assessments.[31]

Context-Specific Regulations on Use of ADMS

In many implementations of ADMS, its regulation will depend on the specific legal and institutional context within which it is deployed. For example, elements of the Code of Criminal Procedure, State Police Manuals and laws which regulate police action in general, will determine how ADMS is used or regulated in police forces; similarly, principles guiding the conduct of elections, located within laws like the Representation of People's Act, will regulate the use of ADMS within those contexts. However, even within these specific contexts where ADMS is widely deployed, there is no translation of broad legal principles into regulatory practice, for example, through rules or regulations around the use or deployments of ADMS. It will be necessary to build on sector-specific and context-specific regulatory frameworks to incorporate necessary protections against ADMS.

There is no single regulatory solution for harmful uses of ADMS in India. However, one important starting point should be to advocate for a strong data protection and private legislation which can incorporate procedural protections against

[25] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Ministry of Electronics and Information Technology, Government of India, (2011) <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>

[26] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

[27] The Aadhaar (Targeted Delivery Of Financial And other Subsidies, Benefits And Services) Act, 2016. (No. 18 Of 2016)

[28] Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Mutual Funds, Securities and Exchange Board of India (2019) <https://www.sebi.gov.in/legal/circulars/may-2019/reporting-for-artificial-intelligence-ai-and-machine-learning-ml-applications-and-systems-offered-and-used-by-mutual-funds_42932.html

[29] Loi n° 2016-1321 pour une République numérique (French Digital Republic Act, 2016.

[30] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Article 29 Working Party <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>

[31] Algorithmic Accountability Act of 2019 (As Introduced in the House of Representatives) <https://www.congress.gov/bill/116th-congress/house-bill/2231/all-info>

ADMS. India's long-awaited privacy legislation – the Personal Data Protection Bill, 2019 – is currently being deliberated by members of a Joint Committee of the Houses of Parliament. The Committee has its work cut out for it – the PDP Bill, while progressive on many fronts, suffers from several lacunae and needs to be future-proofed. One aspect that the PDP Bill must account for is whether it is sufficient for an era of 'Artificial Intelligence' and 'Big Data', where personal data is used to predict and control the behavior of individuals.

[Case Study: India's privacy law needs to incorporate rights against the machine [32]]

India's long-awaited privacy legislation – the Personal Data Protection Bill, 2019 – is currently being deliberated by members of a Joint Committee of the Houses of Parliament. The Committee has its work cut out for it – the PDP Bill, while progressive on many fronts, suffers from several lacunae and needs to be future-proofed. One aspect that the PDP Bill must account for is whether it is sufficient for an era of 'Artificial Intelligence' and 'Big Data', where personal data is used to predict and control the behavior of individuals.

Will the PDP Bill curtail the tyranny of the machine? The Bill does, to a large extent, limit the effects of automated decisions, particularly by allowing individuals to control their personal data and its use, as well as structural changes aimed at entities using personal data. In particular, the Bill provides individuals with a (limited) right to access, rectify and erase personal data, which includes inferences for the purpose of profiling. Profiling, in turn, is defined as "any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal." Therefore, the Bill takes express cognizance of profiling of individuals by automated processing and to some degree allows individuals to control such profiling. However, despite such recognition, it provides few protections against the specific harms from automated profiling and decision-making, leaving the Data Protection Authority to specify certain 'additional safeguards' against profiling for only a subset of personal data deemed to be 'sensitive'.

In order to be a robust legislation for our 'AI' era, we need to implement expanded protections against automated decisions. One way of extending such protection would be to draw from the legal tradition of '**due process**', which ensures that decisions affecting individuals incorporate certain procedural guarantees which are essential to ensuring that they are fair and non-arbitrary. These guarantees include the right to obtain a justification or explanation of decisions, the right to obtain information which was used to make the decision, the right to be heard and have one's views incorporated in the decision, as well as the right to contest or appeal a decision. In the absence of such protections, legal mechanisms should exist which ensure that individuals have the right to object to automated decisions and to have such decisions be subject to meaningful human oversight.

However, placing the burden of contesting decisions on affected individuals will not be sufficient. To overcome this burden, data protection law like the PDP Bill could incorporate structural protections to ensure that automated profiling is fair and transparent. These protections may include, for example, regular audits on the data and techniques used in profiling, to ensure its robustness and safeguard against systematic discrimination. Further, the logic or rules of automated processing of data for purposes of proofing must be made transparent by default. Different levels of protection may be offered in different circumstances, according to the potential harm which may be caused to the subject of the decision.

Opaque and unaccountable AI systems are antithetical to our constitutional ideals of privacy. The Supreme Court of India has noted that decisional autonomy – the freedom to make informed choices for oneself – is a core component of the fundamental right to privacy under the constitution.

> ***However, AI systems limit our ability to make such informed decisions by classifying and typecasting us according to their own secret rules. As we hurl headfirst into the age of 'AI', our legal systems must stand up to the task of protecting our privacy and decisional autonomy.***

[32] Excerpt from an article originally published in Medianama, available at

Data and Databases in Automated Decision-Making in India

Automated Decision-Making Systems utilise technologies which perform computational algorithmic operations on data organised within databases. It is crucial to understand the technological architecture of ADMS systems in India, in order to understand the harms these systems pose and how they may be challenged.

Data is the basic unit for the operation of an ADMS system. Databases are organisations of discrete data points, generally to indicate relationships between different data points and values. While databases in various forms have been created and utilised in the past for informing decision making, contemporary networked technologies and digitisation have radically changed the ability to create, process and communicate data.

Technology policy in India has emphasised the need to collect and process 'raw data' as an elemental resource capable of further transformation into intelligence or insight, or a crucial factor in the production of 'Artificial Intelligence'.[33] However, "'raw data' is an oxymoron", and it is necessary to interrogate what 'raw' data actually represents.[34]

> ***The measurement, classification and categorisation of any phenomenon into 'data' and datasets, which is usable and readable by humans and/or machines, is a task of interpretation which always incorporates human judgements, subjectivities and biases.***

The selection of data for collection and aggregation, to the categories the data is grouped into, and how these categories are ultimately perceived for the purpose of making 'data based decisions', reveal the subjectivities inherent in the data that is used within ADMS.

It is therefore necessary to examine, and reflect upon the assumptions and subjectivity of the 'raw data' used within computational systems and AI systems, for what kinds of knowledge about individuals and groups they reflect, and what the implication of relying upon such data within ADMS might be. To understand how ADMS in India are functioning, it is important to look at the forms of data being collected and processed, as well as the methods of databasing being utilised, which form the underlying elements of any such system.

The databasing practices of public agencies in India (including how, and which, data is collected, stored and structured) have long historical lineages, with data on populations being routinely collected through surveys and censuses and collected in databases like the Census of India, or through police station registries – much of which remains paper-based and reliant on manual entry. More recently, digitisation has resulted in an astonishing number of sources from which data can be obtained.

Digital databases include the Ministry of Road Transport's VAHAN database of vehicle registrations[35], or Karnataka's Bhoomi database of digitised land records,[36] as well as any number of records which enumerate citizens and their relationship with the state - from electricity bills to housing registries. Each of these digital databases are suitable for wide-scale use to store and retrieve information with ease.

The ADMS documented in this project reflect a number of diverse databases and databasing practices being used. Some of these demonstrate clear historical antecedents – such as the various crime and criminal databases at state and central levels. Other databases demonstrate techniques of databasing which are specific to newer technologies of data capture and analysis – such as real-time sentiment analysis on social media, or analytics used in facial recognition systems.

Increasingly, the kinds of data that are collected, and the manner in which they are organised are being informed by ADMS, Big Data and AI. Public agencies are progressively using automated tools for the purpose of capturing and storing data within databases. Technologies like 'sentiment analysis', or social media surveillance technologies, crawl through vast amounts of data on the internet, and only capture and store specific information as determined by the software,[37] and without specific human involvement in each instance. Similarly, public agencies are using internet-enabled sensors within various Smart City projects to monitor traffic or environmental conditions to detect and index information programmatically.[38] These technologies are intended to automatically sense and organise particular patterns of data - therefore delegating the task of data selection itself to algorithmic systems.

Digitisation has allowed for increasing amounts of 'data' to be created and stored in a centralised manner, allowing agencies to both easily generate, record and retrieve information from large databases. This has been a major

[33] See for example, The Report of the Committee of Experts on Non Personal Data Governance Framework, supra.

[34] Gitelman, L. 'Raw Data is an Oxymoron', (MIT Press, 2013).

[35] https://vahan.nic.in/nrservices/

[36] https://landrecords.karnataka.gov.in/service2/

[37] Mathews H V, Sinha A., 'Use of Algorithmic Techniques for Law Enforcement' (2020) 55(23) Economic and Political Weekly 7.

[38] 'Pune Smart City installs 50 environmental sensors', Economic Times, (Feb 24, 2020) <https://government.economictimes.indiatimes.com/news/smart-infra/pune-smart-city-installs-50-environmental-sensors/74284275>

achievement of e-Governance policies and reforms over the last two decades particularly, with extensive computerisation of government agencies, including the computerisation of data which the state collects about citizens.

> ***However, many of these databases carry forward historical legacies of inequities and injustice, often obscuring them by treating them as 'raw data' or by formalising and entrenching them as standard categories and classifications.[39]***

[Case Study: CCTNS And The Haunting Legacy of Criminal Tribes]

The Government of India's Crime and Criminal Tracking Network System is an ongoing project to build a digital network infrastructure for policing across India.[40] The system intends to 'connect' the millions of police records and databases which form part of the routine work of law enforcement agencies in India, in order to make data and information practices more secure, consistent and ultimately more central to the work of law enforcement agencies in India. CCTNS includes data from 'real time' sources like sensors, legacy data from police records, and data 'merged' from other databases used by policing and law enforcement.

While the state of CCTNS implementation remains woeful, including databases being populated by junk records,[41] it is being used to provide the digital data to undertake sophisticated 'crime data analytics' at a nation-wide level, which can further inform policing practice. The analytical softwares will build upon and analyse the 'raw data' provided by various police registers, diaries and other records, including criminal records.

These criminal records carry forward and entrench a haunting legacy of historical caste and ethnic discrimination in policing in India. In many states, the practices of criminal databasing have clear historical lineages with the colonial practice of surveilling and criminalising entire castes and tribes, the so-called 'criminal tribes' which were categorised as tribes 'habitually addicted to crime'. This unscientific and deeply prejudiced system of classification continues to shape policing practice in India. Despite the official 'denotification' of criminal tribes, the biases and prejudices of criminality associated with such castes continue within contemporary policing practices, including in the maintenance of routine police records, such as the Rowdy Register maintained by the Tamil Nadu police under its implementation of the CCTNS, the Goonda Registers maintained in the Bihar CCTNS, or 'History Sheeters' registers maintained in Karnataka. Each of these carry forward explicit continuities with the casteist and racial practices of surveilling and punishing 'criminal tribes' and institutionally embedding discrimination, including through the technologies of digital databases.[42]

As systems like Automated Facial Recognition and predictive analytics are built upon these discriminatory categories and databases, we must introspect on what it means to embed these categories into technological infrastructures which assume 'neutral' or 'data-based' decisions as the basis for police practice, and how we can interrogate and challenge these systems which form the basis of ADMS.

Digital databases need to be organised and structured in particular ways, in order to be usable. This process of structuring databases, classifying the data and identifying the relationships between the data values, is known as data modelling. Many contemporary digital databases are being built as 'relational databases', which is a particular model for structuring and retrieving data. Relational Database Management Systems or RDBMS afford for discrete databases to be linked and information to be retrieved across these databases. RDBMS allows databases to be linked through identifying relationships between two or more records with common features. Common elements in databases can therefore be linked for the purpose of querying or for performing operations across multiple disparate databases. More recently, database models like NoSQL are being utilised to deal with unstructured forms of data, particularly 'real-time' data retrieved from multiple sources. [43]

Public agencies in India are progressively seeking to merge or create linkages across databases which earlier existed in silos. Linking disparate databases has been a major use of the Unique Identification Number project in India, which has utilised large relational database solutions including 'MongoDB' and 'MySQL' to store and retrieve the data of more than a billion Indians.[44] By 'seeding' an Aadhaar number into a pre-existing database, the supposedly unique database of UID numbers was linked to existing databases. This was done not only to create a unique profile of an individual, through their links with various databases, but also to identify that each entry within a database of individuals was unique.[45]

Similarly, various databases have been digitised and 'linked' to remove duplicates,

[39] Bowker, G., Star, S.L., 'Sorting Things Out: Classification and Its Consequences', (MIT 1999)

[40] Narayan S, 'What Ails Smart Policing in India?' Proceedings of Data for Policy 2017, <https://zenodo.org/record/884078>

[41] 'Report no.15 of 2020 - Performance Audit of Manpower and Logistics Management in Delhi Police', Comptroller and Auditor General, <https://cag.gov.in/en/audit-report/details/112172>

[42] Satish M, '"Bad Characters, History Sheeters, Budding Goondas and Rowdies": Police Surveillance Files and Intelligence Databases in India' (2011) 23 National Law School of India Review 133

[43] Relational v NoSQL Data, Microsoft, <https://docs.microsoft.com/en-us/dotnet/architecture/cloud-native/relational-vs-nosql-data>

[44] Mishra, P, 'Inside India's Aadhar, The World's Biggest Biometrics Database', <https://techcrunch.com/2013/12/06/inside-indias-aadhar-the-worlds-biggest-biometrics-database/>

[45] Rao U, 'Population Meets Database: Aligning Personal, Documentary and Digital Identity in Aadhaar-Enabled India' (2019) 42 South Asia: Journal of South Asian Studies 537; Cohen L, 'Limn: Duplicate, Leak, Deity' (Limn, 4 March 2016) <https://limn.it/articles/duplicate-leak-deity/>

even in the absence of Aadhaar seeding – for example, the Government of India's subsidy scheme for cooking gas, "Ujjwala", utilises multiple underlying databases including those provided by cooking gas utilities, and the state's own databases of 'Below Poverty Line' residents, to identify similar beneficiaries in the databases.[46] Similar projects for creating relations between pre-existing databases abound within administrative and governance projects. In doing so, ADMS also rely on data collected across contexts and across various social relationships that individuals may have, which are collapsed into a single identity for the purpose of seeing the citizen. These identities then become the basis for performing algorithmic operations, and ultimately, the basis for administrative decisions.

[Case Study: Data Linkages in Samagra Vedika Scheme]

On August 19, 2014, the Government of Telangana conducted the unprecedented exercise of collecting household statistical data across the state, as part of its 'Samagra Kutumba' Intensive Household Survey. Extensive personal information was collected – from assets to health information about individuals in the state.[47]

Subsequently, the Samagra Kutumba survey has morphed into the Samagra Vedika programme (alternatively known as the Samagra Telangana Smart Governance Platform) – a databasing system which allows for the querying of data across 30 Government databases, including utility, land, and vehicle registration databases. According to the Government of Telangana, utilising data across multiple databases has allowed them to create a '360 Degree Profile' of citizens, which has been praised by the Government of India (which has attempted to emulate the practice through the creation of a National Social Registry - a combination of public databases).[48] These databases are held within government administrations, with citizens themselves given no notification of whether they are included within the databases, or how their information is eventually utilised, including within ADMS.

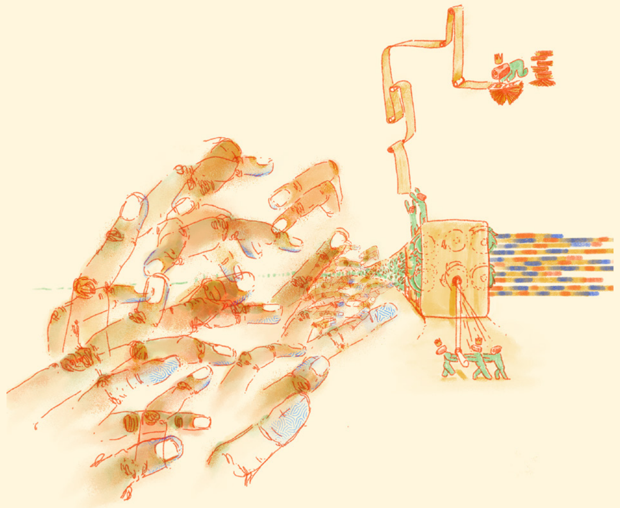
> ***"This is the whole principle of machine learning. There is a concept called ML. The more data you feed, all the inaccuracies are ironed out. This is how it will be. This is the meaning of big data."*** [49]

[46] Muthu GM and Kaur D, 'Ujjwala-Textual and Demographic De-Duplication: Facilitating the PMUY', (2013) <https://informatics.nic.in/uploads/pdfs/a9fdca31_LPG.pdf>

[47] 'Telangana's Samagra Kutumba Survey to Gather Household Details Brings Hyderabad to a Standstill', The Economic Times' <https://economictimes.indiatimes.com/news/politics-and-nation/telanganas-samagra-kutumba-survey-to-gather-household-details-brings-hyderabad-to-a-standstill/articleshow/40812311.cms?from=mdr>

[48] Chitravanshi, R., 'Government working on social registry to better track welfare schemes', <https://economictimes.indiatimes.com/news/economy/policy/government-working-on-social-registry-to-better-track-welfare-schemes/articleshow/56861950.cms?from=mdr>

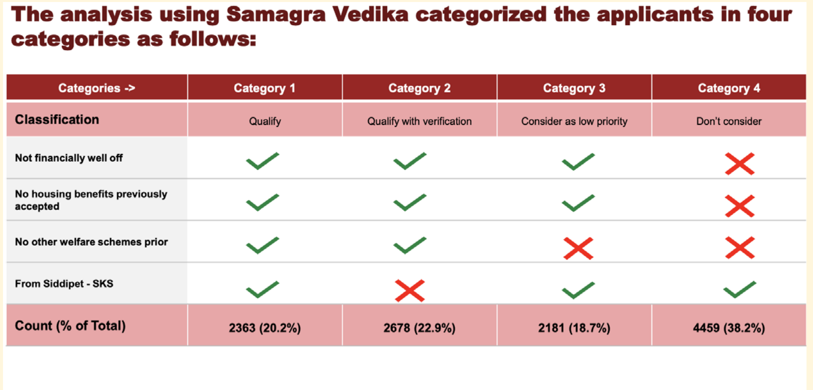
[49] <https://www.medianama.com/2020/09/223-telangana-jayesh-ranjan-interview-facial-recognition/>



This quote is a response from a government official to the possibilities of failure in the machine learning component of Samagra Vedika. It is indicative of the prevalent view within policy and government administration in India, that uncritically assumes that increasing the volume and variety of data used in public administration can lead to improved and objective decision-making, without looking into how data is created, what assumptions and biases it embodies, and what the limitations of its utility are.

The Samagra Vedika system is now being utilised to determine eligibility of residents for welfare schemes, through the use of statistical modelling and 'predictive analytics'. According to publicly available documents, a pilot of the project in Hyderabad to assess the eligibility of welfare beneficiaries led to the removal of 100,000 ration-card holders, ostensibly for being 'ghost beneficiaries' or fraudulent applicants flagged by the system software. After 'public resistance', an appeals and verification process was carried out to reinstate wrongly removed beneficiaries.[50]

Public administrations in India are keen to utilise 'big data' technologies and link databases across sectors and contexts in order to inform their decision-making. The example of Samagra Vedika is indicative of the manner in which database infrastructures are sought to be used by public agencies in India, as well as the possible consequences of utilising this infrastructure without more critical interrogation. With such deference being given to 'data', will people become an afterthought?



The analysis using Samagra Vedika categorized the applicants in four categories as follows:

Categories ->	Category 1	Category 2	Category 3	Category 4
Classification	Qualify	Qualify with verification	Consider as low priority	Don't consider
Not financially well off	✓	✓	✓	✗
No housing benefits previously accepted	✓	✓	✓	✗
No other welfare schemes prior	✓	✓	✗	✗
From Siddipet - SKS	✓	✗	✓	✓
Count (% of Total)	2363 (20.2%)	2678 (22.9%)	2181 (18.7%)	4459 (38.2%)

[50] Samagra Vedika, Telangana's Integrated Platform, ITE&C Department, Government of Telangana <http://pubdocs.worldbank.org/en/945071576869997489/GT-Venkateshwar-Rao-Presentation-on-Samagra-Vedika-to-Wordl-Bank-seminat-Dec-19.pdf>

Algorithms and Automated Decision-Making Systems in India

An algorithm, in its essence, is a set of rules, or a series of steps, to be followed in any method for reaching a particular output from a given starting point. This toolkit documents and analyses computational algorithms – methods and processes followed within computational processing of data to generate outputs, which are ultimately used within Automated Decision Making Systems, to make consequential decisions. While algorithms vary in form and nature, there are some general characteristics of algorithms which can inform the approaches we take towards addressing the concerns of ADMS use in India.[51]

> ***Algorithmic systems encode particular forms of knowledge and logic, including biases and assumptions about the behaviour of individuals and society. These systems are particularly important to study because these logics become embedded within computational and networked infrastructure which is replicated and operates at scale and speed - affecting large populations and creating systemic changes, often without the foresight or caution to understand and mitigate their potential harmful consequences.***

The 'worldview' of an algorithm is context-specific, inheriting the knowledge and biases of the designers of the technology. Notwithstanding claims of 'general artificial intelligence' likening AI to human intelligence, algorithms are limited by the assumptions on the basis of which they have been designed. They operate and identify only on particular representations of digital data, and extract only such meaning from that data as they have been designed to. The failure to understand these limitations has led to concerning forms of 'technological solutionism' within institutions of law and governance.

[51] Gillespie T, 'The Relevance of Algorithms' in Tarleton Gillespie, Pablo J Boczkowski and Kirsten A Foot (eds), Media Technologies (The MIT Press 2014) <http://mitpress.universitypressscholarship.com/view/10.7551/mitpress/9780262525374.001.0001/upso-9780262525374-chapter-9>

[Case Study: Automated Censorship In Online Platforms]

In December, 2018, the Government of India made public draft rules for regulating online platforms, the draft 'Intermediary Guidelines Rules, 2018'.[52] Among other things, the rules contained one particularly concerning mandate – Rule 3(9) requires all intermediaries to deploy 'technology based automated tools' to proactively identify and disable 'unlawful information'. Besides being vague and over-broad, the rule indicates the increasing proclivity of public agencies to assume that 'automated tools' – essentially, algorithmic systems – are capable of performing complex tasks which inherently involve human judgement – including the ability to identify information which may be unlawful. The problem with these assumptions is the failure to recognise the limitations of algorithmic systems operating in complex, human, contexts.

Determining the legality of information requires understanding the context in which it appears – whether it is intended as a parody, is a quotation, or if its meaning depends on the group that uses it – contexts which algorithmic models today, cannot understand.[53] Instead, most contemporary algorithmic filters merely look for particular phrases, combinations of words or images, and automatically flag or censor any information which matches these – a process known as 'fingerprinting'. This is not the first time that public agencies have attempted to use algorithmic systems to censor online content. In 2018, the Central Bureau of Investigation requested social media platforms to deploy an automated content identification system called PhotoDNA,[54] which uses fingerprinting technology to identify photographs and disable their access. While fingerprinting can work in specific, limited contexts – for example, in preventing child sexual exploitation images – its use across contexts risks the pre-censorship of legitimate and lawful speech. Ultimately, the failure to recognise the limitations of 'AI' tools and automated censorship can lead to unjustified restrictions on important rights, without scientific or legal legitimacy.

[52] Draft Intermediary Liability Guidelines (Amendments) Rules, 2018, <https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf>

[53] Llansó EJ, 'No Amount of "AI" in Content Moderation Will Solve Filtering's Prior-Restraint Problem' (2020) 7 Big Data & Society.

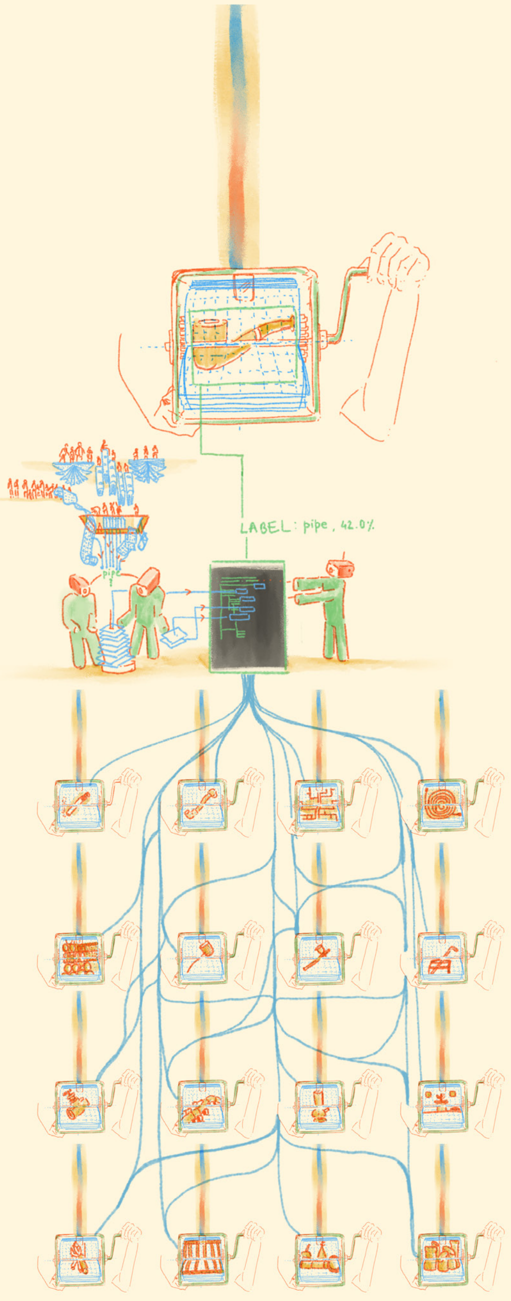
[54] Singh, S., 'CBI Asks Social Media Firms to Use Intrusive Photo Tech to Track Suspects,The Indian Express' <https://indianexpress.com/article/india/cbi-surveillance-photodna-microsoft-facebook-youtube-twitter-5516347/>

The application of algorithms requires the **definition of a problem**, and the specification of the output which is desired in a manner that can be produced by the algorithmic process. This requires a problem to be formalised in terms of measurable and quantifiable inputs and outcomes. For example, in an algorithm where the question posed is 'determining fraudulent behaviour in taxation', the formalisation could be a desired output based on a 'ground truth' which states that 'outlying patterns of differences in declared income and expenditure indicate fraudulent behaviour'. Once the problem has been formalised in this manner, a fraud detection algorithm can be designed to study patterns which match the description of the pattern and classify transactions as 'fraud' or 'not fraud'. The problem definition is an aspect of algorithmic modelling which makes human judgements and values most explicit. For example, in an ADMS which decides whether a person is 'potentially criminal', requires the designers of an algorithm to determine what qualities of an individual can be mathematically calculated in order to identify their 'criminality', which necessarily incorporates subjective judgements about people's behaviour.[55]

The **nature of the algorithm** used indicates the kind of logic that is applied in coming to a particular decision. Algorithms can be grouped according to the general mathematical or statistical approaches they take towards solving a particular problem (or reaching the desired, pre-defined output). Some of the historical examples of early AI used by public agencies were 'logic based' expert systems, which were programmes in the form of 'if/then' statements, or deterministic paths to follow from a particular input. On the other hand, many contemporary algorithmic models utilise machine learning.[56]

Machine learning is a set of algorithmic systems, which recognises underlying patterns in data to understand correlations between data, or to model and 'predict' the behaviour of future instances of data.[57] Machine learning algorithms are some of the most widely used in ADMS today, including the systems documented here. Machine learning systems, in particular, are increasingly popular as methods to sort through vast amounts of information to identify patterns which may not be immediately obvious to humans. Machine learning models learn from historical instances of data that they are 'trained' on. Because machine learning merely reproduces and optimises certain relationships from historical data, the uncritical reliance on machine learning techniques to inform decision-making can reproduce systemic biases and structural inequalities present in underlying historical data.

The nature of the algorithm can impact not only its utility towards solving a particular problem, but also other important elements around the design of ADMS – such as the ability of the system to be scrutinised, or limitations in its ability to factor in important values like non-discrimination or other constraints. For example, decisions which utilise a linear regression model, which maps relationships between independent variables, may be easier to explain to users of the system, than those which utilise multi-layered neural network models, such as those seen in contemporary facial recognition systems, including those widely used by law enforcement in India.[58] In the previous example of an algorithm for determining fraudulent tax payments, a series of legal rules may be encoded into an expert system which determines whether the input data, as processed by the rules provided to it, indicate fraud. Alternatively, in the case of a machine learning system, the algorithm may be 'trained' on previously established cases of 'frauds' to find patterns and correlations which can be applied to subsequent cases in order to classify them as 'fraud' or 'not fraud'.



The task of selecting the algorithm to be applied for a particular problem also requires subjective judgements – what kinds of error rates (false positives or false negatives in the output) are acceptable given the constraints of computing power and time? What is a suitable threshold for statistical bias and variance exhibited by a machine learning algorithm?

A second important component of algorithmic design is **data**. Computational algorithms operate on specific **databases**, within which particular data has been structured and organised. Some of the forms of data and databases used in ADMS in India have been discussed here. As discussed previously, for data to be suitable for computation, data must be classified, structured and organised in particular ways.

[55] Barocas S and Selbst AD, 'Big Data's Disparate Impact', 104 California Law Review 671 (2016).

[56] Lehr D and Ohm P, 'Playing with the Data: What Legal Scholars Should Learn About Machine Learning' 51 UCD L. Rev., 651.

[57] Mitchell, T., 'Machine Learning', (McGraw Hill, 1997).

[58] Burrell J, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society

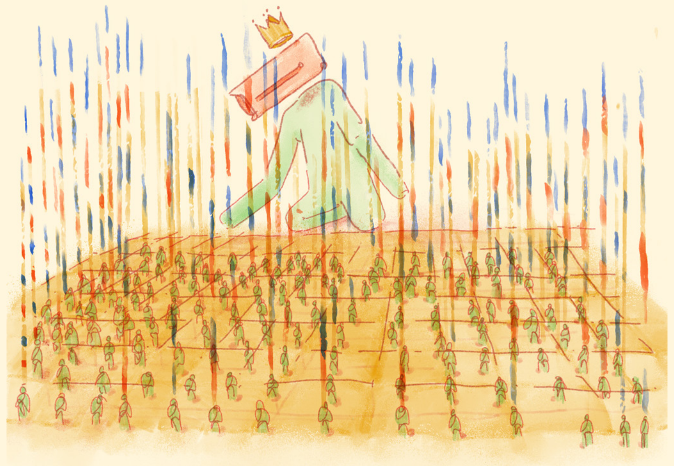
Various kinds of databases can go into the operation of a single ADMS. In a Machine Learning system, one database from which the algorithmic model 'learns' is known as a training database. The 'trained model' is often evaluated against a different database to judge its efficacy, through a 'benchmark database'. Finally, the model operates on 'new' databases which it has not previously encountered, at the point of deployment. Each of these databases ultimately impacts how an algorithm performs, as well as how it is evaluated or audited. For example, when a Machine Learning process is identified as being 'accurate', it is essential to understand the conditions and context in which the algorithm has been tested, and against what kinds of benchmark datasets.[59] Reliance on algorithms for decision-making can reproduce and magnify inaccuracies or biases at scale, particularly when these algorithms are deployed by public agencies which interface with large populations. Even relatively 'simple' algorithmic processes are embedded within complex socio-technical systems of actors, institutions, norms, organisations and technical components, making the operation of algorithms 'on the ground' difficult to predict, and making responsibility for inaccuracies or problems in the design of the algorithm difficult to understand or study.

[Case Study: Algorithmic Assemblages and the Ghosts in India's Welfare Machine]

The Aadhaar Unique ID project of the Government of India is based on the presupposition that digital databases can represent the ground truth of unique individual identities – a necessary element in the projects claims towards removing 'leakages' by removing 'duplicates' – the title given to potentially fraudulent actors or 'ghosts' who siphon off the legitimate claims of welfare beneficiaries. Making digital records 'unique' has therefore always been the claim and the purpose of the biometric ID. These claims of uniqueness are made possible by the assemblages of algorithmic systems utilised within the Aadhaar ADMS.

Biometric algorithmic systems form the core of Aadhaar's enrolment and authentication mechanism. A device captures fingerprints, iris scans and face images, and encodes it as an apparently unique digital imprint, by extracting particular patterns and signals from the captured biometric features. These patterns are then matched and compared with existing entries in the biometric database, in order to identify similarities according to a pre-defined threshold. Aadhaar claims to 'authenticate' individuals by matching the data captured through a biometric device at any point, to the data stored in the central biometric database. While the UIDAI claims that its biometric matching algorithms are highly efficient and accurate, by the government's own admission, the 'failure rate' of the system is as high as 12%,[60] although it is not clear whether this is attributable to how the data is measured, or how it is matched with other entries in the database.

Another algorithmic component of Aadhaar has been the 'seeding' of Aadhaar numbers within multiple other databases, in order to identify and remove duplicates – in a process known as 'de-duplication'. According to the UIDAI, the authority in charge of Aadhaar, "De-duplication is the process of using the Demographic and Biometric data collected from an enrollee to check against rest of the data so as to avoid duplicate enrolments.[61]" De-duplication algorithms perform 'inorganic' seeding by matching names in various welfare beneficiary databases to the Aadhaar numbers database. If the algorithm does not find a match, it is assumed that the beneficiary entry is a 'ghost' or a 'fake', if there is more than one match, the beneficiary is assumed to be a 'duplicate', and consequently, removed from the list of beneficiaries. The output of the algorithmic computation, then, is privileged over the claims of the affected persons, or even the administrative officials on the ground.



Every stage of Aadhaar's decision-making process relies on the design of, and values, biases and errors embedded within the algorithms and technologies utilised within Aadhaar – from the sensitivity of the biometric recognition and matching algorithms to biometrics of different demographics, to the error rates of the 'seeding algorithms' for de-duplication. Even as these algorithms have repeatedly been shown to be prone to failure and error, government processes continue to rely heavily on their 'objectivity' of algorithmic systems, without designing for how these failures can be contested or overturned by affected persons.

[59] Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018

[60] 'Aadhaar Authentication for Govt Services Fails 12% of Time: UIDAI', The Quint, (March 27, 2018) <https://www.thequint.com/news/india/uidai-ceo-admits-aadhaar-authentication-failure-rate-12>

[61] Role of Biometric Technology in Aadhaar Enrollment', UIDAI, <http://www.dematerialisedid.com/PDFs/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf>