UNDERSTANDING INSTITUTIONAL AI

(Artificial Intelligence)

SECTORAL CASE STUDIES FROM INDIA

By Anulekha Nandi

GLOBAL NETWORK INITIATIVE
Internews
US-INDIA POLICY INSTITUTE
DEF DIGITAL EMPOWERMENT foundation

Understanding Institutional AI: Sectoral Case Studies from India

Working Paper

February 2020

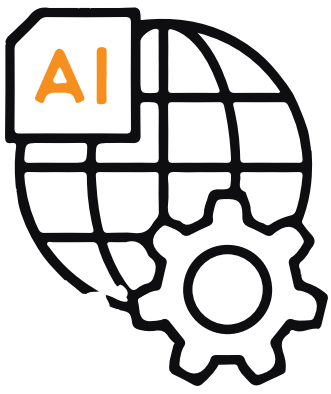
Author: Anulekha Nandi

Design and Layout: Satish Kumar

You can read the online copy at www.defindia.org/publication-2

Digital Empowerment Foundation
House no. 44, 2nd and 3rd Floor (next to Naraina IIT Academy)
Kalu Sarai (near IIT Flyover)
New Delhi – 110016
Tel: 91-11-42233100 / Fax: 91-11-26532787
Email: def@defindia.net | URL: www.defindia.org

CONTENT

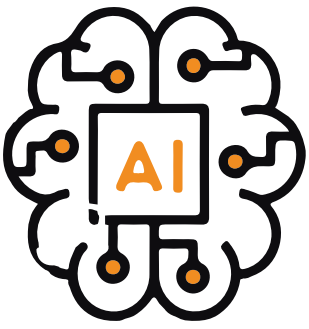


INTRODUCTION

India ranks 3rd in the Asia Pacific region on Artificial Intelligence (AI) readiness after Singapore and Hong Kong according to a Salesforce study[1]. India ranked 3rd among G20 countries in 2016 on the number of AI focused start-ups which have increased at a compound annual growth rate of 86% higher than the global average[2]. According to a study by Accenture, AI has the potential to add $957 billion or 15% of the gross value added to India's economy by 2035[3]. Though the AI market in India is estimated to grow to $89.8 billion by 2025, it continues to be underinvested by risk capital investors compared to competition in the US and China[4].

However, the Indian ecosystem has its limitations in providing an enabling environment for AI due to lack of quality data and reliable datasets. Despite these limitations coupled with challenges of India's demographic and linguistic diversity, venture capitalist firms to report that 25-30% of the proposals they received contain a significant AI component[5]. Further, companies that have managed to raise capital and establish their business are seeing positive traction and expansion not just domestically but also internationally[6]. Alongside the proliferation of proprietary technology and start-ups incorporating AI in their service delivery there are institutional applications of AI through public-private partnerships (PPPs) that aim to extend the application of the technology towards improving social sector outcomes. While in some sectors such deployments have taken the course of pilots through PPP arrangements, in others they have moved towards policy alignment and laying the foundations to springboard such interventions, while in some others it has moved towards significant adoption and deployment.

One of the recurring felt needs articulated by different policy documents is the lack of data infrastructure/architecture on the back of which AI applications can be deployed and scaled. Sectoral policy documents have articulated different forms of data integration and database linkages however, the unified idea seems to be that of IndiaStack undergirded by Aadhaar and the proposed JAM trinity[7] [8]. Given the direction of sectoral policies to interlink and aggregate databases under their purview this has the potential to provide a data driven 360 degree view of an individual within administrative institutions. However, this potentiality is not circumscribed by legal safeguards that can provide either sectoral or general purpose protections against misuse and move towards a standard measure for transparency, accountability, safety, security, and due diligence in protecting individuals from risk of harms.

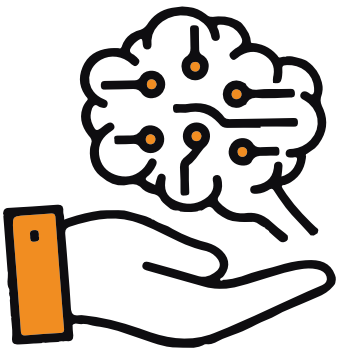


[1]EC Bureau. (2019). Indian third in APAC on AI readiness. Economic Times. Retrieved from https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/india-third-in-apac-in-ai-tech-readiness/articleshow/68805284.cms?from=mdr [16 Feb 2020]
[2]Sachitanand, R. (2019). Here's why Indian companies are betting big on AI. Economic Times. Retrieved from https://economictimes.indiatimes.com/tech/internet/heres-why-indian-companies-are-betting-big-on-ai/articleshow/67919349.cms?from=mdr [16 Feb 2020]
[3]Ibid.
[4]Ibid.
[5]Ibid.
[6]Ibid.
[7]TAGUP. (2011). Report of the Technology Advisory Group for Unique Projects. Retrieved from https://www.finmin.nic.in/sites/default/files/TAGUP_Report.pdf [28/11/2018].
[8]The JAM trinity refers to triangulation of data through the Aadhaar database, mobile numbers, and Jan Dhan social protection scheme for financial inclusion.

THE AI POLICY LANDSCAPE IN INDIA

The Indian digital policy and regulatory landscape is awash with initiatives to mainstream (AI) in key social and economic infrastructures. The National Strategy for Artificial Intelligence released by NITI Aayog (the Indian government's policy think-tank) in June 2018, underscores the government's policy intent to mainstream AI in healthcare, agriculture, education, smart cities and infrastructure, and smart mobility and transportation[9]. The Artificial Intelligence Task Force (AITF), constituted by the Ministry of Commerce and Industry, has identified 10 focus areas to use AI to work on institutional gaps plaguing those sectors. These include manufacturing, FinTech, healthcare, agriculture/ food processing, education, retail/ customer engagement, accessibility technology for differently abled, environment, national security, and public utility services[10].

The Ministry for Electronics and Information Technology constituted four committees for promoting AI initiatives and developing policy framework: (1) Committee A on platforms and data for AI; (2) Committee B on leveraging AI for identifying national missions in key sectors; (3) Committee C on mapping technological capabilities, key policy enablers required across sectors, skilling and re-skilling, and R&D; (4) Committee D on cyber security, safety, legal and ethical issues[11]. Committee B identified 17 key sectors that would require national AI missions for infusing technology enabled efficiency[12]. These multiple initiatives by different government departments highlight the deepening ethical, legal, and technological complexity of India's chequered artificial intelligence landscape. It also demonstrates a move towards adoption, uptake, and deployment of AI in critical social, economic, and governance sectors by government and administrative institutions.



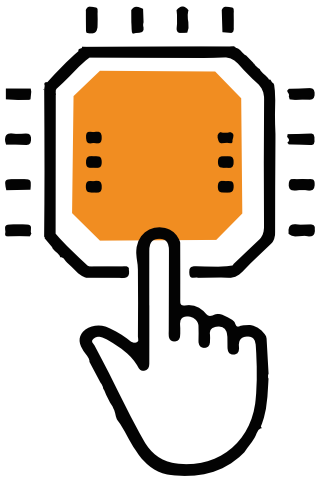
[9]NITI Aayog. (2018). National strategy for artificial intelligence. Retrieved https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf [16 Feb 2020].
[10]DIPP. (n.d.). Report of task force on artificial intelligence. Retrieved from https://dipp.gov.in/whats-new/report-task-force-artificial-intelligence [16 Feb 2020].
[11]MEITY. (n.d.). Artificial intelligence committee reports. Retrieved from https://meity.gov.in/artificial-intelligence-committees-reports [16 Feb 2020].
[12]MEITY. (2019). Report of committee B on leveraging AI for identifying national missions in key sectors. Retrieved from https://meity.gov.in/writereaddata/files/Committes_B-Report-on-Key-Sector.pdf [16 Feb 2020].

PROPOSED DATA GOVERNANCE FRAMEWORK

The current data protection framework in the shape of the Personal Data Protection Bill, 2019 which presently stands referred to a Joint Committee does not contain any specific reference to automated decision making. While the risk of harms delineated therein can be extended to provide protection against risks generating out of automated decision-making their application would remain the prerogative of the Data Protection Authority whose appointments are at the discretion of the Central Government. Given that the Central Government also has the authority to exempt any agency of the government from the application of the Data Protection Act, this undermines the independence with which the Authority should be able function and act as an independent oversight body, particularly in cases of mass data collection for intelligence and law enforcement purposes.

Compounding this are the significant carve outs for non-consensual processing (section 12) for government functions as well as exemptions which allow the Central Government to exempt any agency of the government from the Act (section 35) as well as for personal data "processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force" (section 36a)[13]. This nullifies any protection or recourse offered by the law to the data subject or data principal as they are referred to the in the Indian context. This makes the conditions for the data subject/ principal under special institutional arrangements like PPPs even more precarious, especially because they pertain to sensitive personal information (as in the case of health), particularly with regard to marginalised and underserved communities (as in the education), as well as mas collection of biometric information and interlinkage of multiple databases (as in the case of law enforcement).

This raises questions about the balancing between general purpose principled consideration for AI application and sectoral specificities. With AI being a general purpose technology its application in different sectors engenders specific risk interfaces that require contextual understanding and application of principles, however there are certain common consideration that can be extrapolated across sectoral applications that require unified basis of principled operations. This report looks at cases of sectoral applications of institutional AI in India in order to understand the sectoral specificities as well the commonalities across these cases. In the absence of strong legal frameworks, it attempts to look at how a business human rights framework can act as guiding resource towards future policy-making in this area.



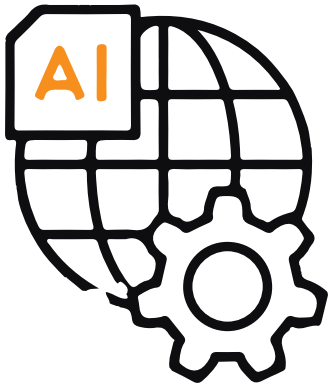
[13]Personal Data Protection Bill. (2019). Retrieved from http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf [16 Feb 2020].

SELECTION OF CASES

This report focuses on cases in education, health, and law enforcement because they (a) represent different stages of institutional application of AI and the incidence of impact on privacy for different sections of the citizenry as well as (b) the different types of institutional arrangement with private service providers; while at the same time (c) the different categories of data used and datasets used, proposed to be used, linked, and combined. The case studies help to provide an indication of the contours shaping each sectoral application while helping to understand the common foundational safeguards wanting in each. The case studies are not meant to be exhaustive but indicative since there are a number of sectoral applications that have not been included within this report.

These include sectoral applications in agriculture where Microsoft has partnered with ICRISAT to develop an AI Sowing App powered by Microsoft Cortana Intelligence Suite including machine learning and Power BI as well as a partnership by Microsoft[14] and the Karnataka government in using predictive analytics in forecasting of commodity pricing[15]; application in smart city, transportation, and smart mobility that run an entire gamut of using facial recognition technology for public safety and deployment of AI for transportation management and road safety[16] [17]; governance and administration where the National Informatics Centre has developed a project that uses AI to monitor the progress of toilet construction under the Swachh Bharat Abhiyan (Clean India Campaign). The project claims to detect location and identity of the beneficiary through facial recognition technology and the physical condition of the toilet from the pictures taken through a GPS-enabled smartphone[18]. And the only way the government would be able to match the facial recognition data is against the Aadhaar biometric database since the Aadhaar details of beneficiary are taken for direct transfer of benefits to individual to build toilets in their homes in order to make India open defecation free.

While each of these cases merit a closer look the case studies selected for this report are meant to serve as an indicative analysis of the areas of application where accountability and due diligence standards would most serve to enhance transparency and develop further exploratory and investigative studies across various sectors that aim to move towards holistic understanding of the multi-dimensional issues and considerations engendered by contextual and sectoral applications of AI.



[14]NITI Aayog. (2018). National strategy for artificial intelligence. Retrieved https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf [16 Feb 2020].

[15]Nagpal, J. (2017). Government of Karnataka inks MoU with Microsoft to use AI for digital agriculture. Retrieved from https://news.microsoft.com/en-in/government-karnataka-inks-mou- microsoft-use-ai-digital-agriculture/ [16 Feb 2020].

[16]see for example, Business Standard. (2015). Microsoft brings together start-ups to offer solutions for smart cities. Retrieved from https://www.business-standard.com/article/companies/microsoft-brings-together-start-ups-to-offer-solutions-for-smart-cities-115100600982_1.html [16 Feb 2020].

[17]Basu, A. & Hickok, E. (2018). Artificial intelligence in the governance sector in India. Centre for Internet and Society. Retrieved from https://cis-india.org/internet-governance/ai-and-governance-case-study-pdf [16 Feb 2020].

[18]Prasad, R.S. (2018). 'Applying AI in governance will let India leapfrog many developmental, infrastructural constraints'. Economic Times. Retrieved from https://economictimes.indiatimes.com/tech/software/applying-ai-in-governance-will-let-india-leapfrog-many-developmental-infrastructural-constraints/articleshow/64020506.cms?from=mdr [16 Feb 2020].

NATIONAL AND INTERNATIONAL LANDSCAPE ON AI POLICY, DATA GOVERNANCE, AND CORPORATE ACCOUNT-ABILITY

Technology has come to be inextricably integrated within social and economic life such that epithets like 'digital economy' would soon become obsolete since there would be no economy without its digital element. With companies and businesses being the core suppliers of this critical component it becomes increasingly important to understand how their operational practices, the technologies that they build, and the modalities of the technologies themselves inflect the social and economic opportunities and fundamental rights of citizens for whom such technologies are deployed. Given that the risk of harms under automated technologies are pervasive, invisible, and structural it makes the task of evidence-based accountability and grievance redressal under a business and human rights framework complex to unravel. Compounding this fact are the diversity of contexts and sectors within which such technologies are deployed which require contextual nuances to be effective.

The United Nations Guiding Principles on Business and Human Rights (UNGPBHR) recognised the role played by corporates as an important stakeholder in respecting and preserving human rights within areas in which they operate and to be held accountable in instances of their violation. The UNGPBHR provide an important framework for delineating human rights within the twin pillars of duty of the State to protect and the responsibility of the businesses to respect human rights complemented by the third pillar of providing access to remedy[19]. However, in order to operationalise the framework it is important to integrate its application within safeguards offered by national laws along with their obligation towards international human rights commitments to serve as a guiding document for policy-making.

It is also important to recognise the advancements made in arriving at ethical principles for automated decision-making by multi-stakeholder and multi-lateral fora like the OECD Principles on AI, European Commission Ethical Guidelines for Trustworthy AI, as well as the Toronto Declaration: Protecting the Right to Equality and Non-Discrimination in Machine Learning Systems. Further, it is important to recognising the crystallisation of international human rights standards like the Universal Declaration of Human Rights; International Covenant of Civil and Political Rights; and International Covenant on Economic, Social, and Cultural Rights into the GNI (Global Network Initiative) Principles and their specific application to technology companies. However, concurrently, in order to operationalise and contextualise the above frameworks and principles it is also important to recognise national articulations of privacy within the landmark *Puttaswamy* judgement that held privacy to be a constitutionally guaranteed fundamental right as well as the privacy harms envisioned by the proposed Personal Data Protection Bill, 2019.

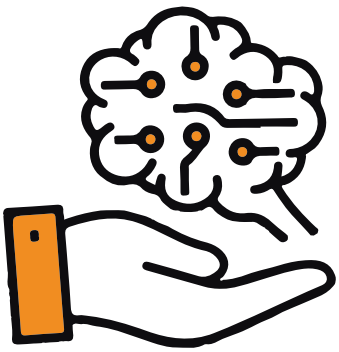
[19]United Nations Human Rights Officer of the High Commissioner. (2011). Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect, Remedy" framework. United Nations. Retrieved from https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf [16 Feb 2020].

With the multi-dimensional impact of automated decision-making and its potential for pervasive impact on privacy rights of individuals it helps to delineate the risk of harms attendant on the erosion of privacy through re-purposing, interlinkage,and combination of data and datasets.

The central proposition of the *Puttaswamy* judgement held privacy to be protected as an intrinsic part of right to life and liberty under Art.[20] and as a part of freedoms guaranteed by chapter III of the Indian Constitution which lists the fundamental rights guaranteed to every citizen in India and includes the rights to equality, right against discrimination, and right to freedom of expression etc. Further, the Personal Data Protection Bill, 2019 aims to protect the rights of the individuals whose data are being processed and provide remedies for unauthorised and harmful processing where harm include (*i*) bodily or mental injury; (*ii*) loss, distortion or theft of identity; (*iii*) financial loss or loss of property; (*iv*) loss of reputation or humiliation; (*v*) loss of employment; (*vi*) any discriminatory treatment; (*vii*) any subjection to blackmail or extortion; (*viii*) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (*ix*) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (*x*) any observation or surveillance that is not reasonably expected by the data principal[21].

The GNI Principles place positive responsibilities on businesses to protect the privacy rights of their users with respect to personal information and work to respect and "protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards"[22]. With the multi-dimensional impact of automated decision-making and its potential for pervasive impact on privacy rights of individuals it helps to delineate the risk of harms attendant on the erosion of privacy through re-purposing, interlinkage, and combination of data and datasets. Without adequate safeguards this might lead to pervasive discrimination against already marginalised and underserved groups. Thus, balancing of innovation, right, and accountability both in principle and design[23] become crucial to ensure in order to work towards inclusive AI systems that include human oversight along with technical safeguards within a robust privacy and data protection framework that ensure diversity, non-discrimination and fairness provides transparency and accountability[24].

In moving towards responsible business application of automated decision-making it becomes important to ensure application of principles not just to the expected outcomes of automated decision-making but also to algorithmic processes to ensure data selection and inputs, hypotheses, and inferences follow a progressive rights-protective approach that



[20]Devadasn, V & Bhatia, G. (2017). The Supreme Court's right to privacy judgement - I: Foundations. Retrieved from https://indconlawphil.wordpress.com/2017/08/27/the-supreme-courts-right-to-privacy-judgment-i-foundations/ [16 Feb 2020].
[21]Personal Data Protection Bill. (2019). Retrieved from http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf [16 Feb 2020].
[22]GNI. (2019). GNI principles. Retrieved from https://globalnetworkinitiative.org/gni-principles/ [16 Feb 2020].
[23]from OCED. (2019). OECD principles on AI. Retrieved from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [16 Feb 2020].
[24]from Independent High Level Group on Artificial Intelligence. (2018). Ethics guidelines for trustworthy AI. European Commission. Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation [16 Feb 2020]

In moving towards responsible business application of automated decision-making it becomes important to ensure application of principles not just to the expected outcomes of automated decision-making but also to algorithmic processes to ensure data selection and inputs, hypotheses, and inferences follow a progressive rights-protective approach that work to mitigate the risk of harms.

work to mitigate the risk of harms. Concomitantly, with business responsibility for inclusive AI the state's duty to ensure the protection of rights within automated decision-making also become crucial to develop a principled systems. This becomes especially significant within hybrid institutional arrangements like PPPs which contend the gaps between rights and exemptions within proposed legal safeguards like the Personal Data Protection Bill, 2019. Thus, it becomes incumbent upon the State to reduce harms within public sector systems by identifying risks, ensuring transparency and accountability, promoting equality through proactive measures and holding private sector to account[25]. This balancing of the state duty and business responsibility to protect human rights will help to move towards an ecosystem of progressive innovation that respects that rights of those for whom and on whose data such systems are predicated.

[25]from The Toronto Declaration. (2018). The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems. Access Now. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf [16 Feb 2020].

AI

(Artificial Intelligence) in Education in India

Questioning Justice And Inclusion

ARTIFICIAL INTELLIGENCE IN EDUCATION IN INDIA: QUESTIONING JUSTICE AND INCLUSION

Introduction

The National Strategy for Artificial Intelligence, released by NITI Aayog (the Indian government's policy think tank) in June 2018, underscores the government's policy intent to mainstream artificial intelligence (AI) in critical social and economic infrastructures[26]. Out of the 10 focus areas identified by the Artificial Intelligence Task Force, constituted by the Ministry of Commerce and Industry[27], the education sector has seen the most successful public-private partnerships (PPPs) to deal with some of the institutional gaps plaguing the sector[28].

With AI being a data-hungry technology, it becomes increasingly problematic when it is trained on the sensitive personal information of marginalised populations through service delivery in key social infrastructures like education. This is especially concerning given the current lack of a data protection regulation in India and the concomitant carve-outs for state functions in public service delivery. Moreover, the draft data protection bill which is currently tabled before the parliament does not contain explicit provisions on algorithmic decision making, including the right to be informed of its existence and the right to opt out, unlike the European Union's General Data Protection Regulation (GDPR)[29].

The impetus behind the deployment of AI has outstripped legal and regulatory development in the area, leaving a governance vacuum over a general-purpose technology with unquantifiable impact on society and economy. Given the multidimensional and cross-cutting risks and opportunities that this poses, along with complex and dynamic ethical challenges, it becomes imperative to study and understand use cases to inform and work towards context-sensitive AI governance frameworks.

Institutional AI in the Indian technology and education paradox

The use of technology in education in India traverses the unequal realities of two facets of the country. On one hand there is the

[26]NITI Aayog. (2018). National Strategy for Artificial Intelligence. New Delhi: NITI Aayog. https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
[27]DIPP. (n.d.). Report of task force on artificial intelligence. Retrieved from https://dipp.gov.in/whats-new/report-task-force-artificial-intelligence [16 Feb 2020].
[28]NITI Aayog. (2018). National Strategy for Artificial Intelligence. New Delhi: NITI Aayog. https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
[29]Das, S. (2018, 30 July). 8 differences between Indian data protection bill and GDPR. CIO & Leader. Retrieved from https://www.cioandleader. com/article/2018/07/30/8-differences-between-indian-data-protection-bill-and-gdpr [16 Feb 2020].

Institutional applications of AI are based on public data collected by the government through service delivery, especially with regard to the social protection of marginalised, underserved and vulnerable populations, and are not undergirded by the need for adherence to data protection principles

segment of the population with access to digital, social and economic resources and on the other there is the vast majority for whom even basic institutions of social infrastructure offer rudimentary support at best. Private investment in education technology – or EdTech – is a burgeoning industry which clocked a valuation of USD 4.5 billion globally in 2015[30]. As per data from the research firm Tracxn, out of the 300 Indian start-ups that use AI as a core product offering, 11% are based in the education sphere[31]. India's digital learning market was valued at USD 2 billion in 2016 and is projected to grow at a compound annual growth rate (CAGR) of 30% to reach USD 5.7 billion by 2020[32]. However, the product offerings that result from these significant investments either aim to offer tutoring services, improve learning outcomes, or provide customised learning, all of which serve to leverage and augment the agency of the first segment of the population. The uptake, adoption and usage of these services proceed through the notice and consent protocols of informed consent due to service requirements of digital distribution platforms like Android's Google Play Store or Apple's Apple Store.

However, institutional applications of AI are based on public data collected by the government through service delivery, especially with regard to the social protection of marginalised, underserved and vulnerable populations, and are not undergirded by the need for adherence to data protection principles. Moreover, a joint reading of the draft data protection bill and judgement of the Supreme Court on the use of Aadhaar biometric information[33] for exercising state functions of public service delivery highlights the exemptions from informed consent or other complementary data protection protocols for state functions aimed at social and economic inclusion. This begs the question as to how the sensitive personal data of citizens, especially of the marginalised, are to be protected within institutional applications of AI through PPP arrangements which lack transparency on the commercial service commitments, data protection protocols and safeguards, data-sharing arrangements and processes of labelling and annotation. These are further compounded by the gaps in explainability, framing, deployment and application.

[30]NITI Aayog. (2018). National Strategy for Artificial Intelligence. New Delhi: NITI Aayog. https://niti.gov.in/writereaddata/files/document_ publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
[31]Khera, S. (2019). Artificial intelligence in education in India, and how it's impacting Indian students. The News Minute. https://www.thenewsminute.com/article/artificial-intelligence- education-and-how-its-impacting-indian-students-95389 [16 Feb 2020].
[32]NITI Aayog. (2018). National Strategy for Artificial Intelligence. New Delhi: NITI Aayog. https://niti.gov.in/writereaddata/files/document_ publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
[33]The Aadhaar is a 12-digit unique identification system based on biometric information and demographics issued to an Indian resident. It is governed by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.It became controversial when mobile phone service providers and banks started asking for the card as a condition for using their services. More problematically, it became conditional for the delivery of critical social protection schemes like midday meals to underserved students, availing rationed food items, pension schemes, etc., in some cases with people denied these services dying. The card was the subject of cases filed before the Supreme Court of India which challenged its constitutional validity due to its privacy infringing features and that it was being required to access private sector services. Though the Supreme Court upheld the fundamental right to privacy, in September 2018 it also upheld the constitutional validity of the identification system in that it allowed Aadhaar-based authentication for establishing the identity of an individual for receipt of a subsidy, benefit or service provided by the government by retaining section 7 of the Aadhaar Act that allows for welfare to be made contingent on the production of Aadhaar.

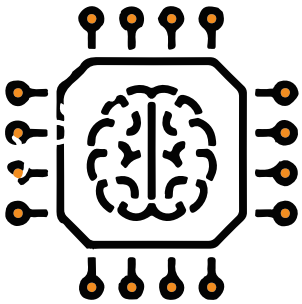
One of the most pervasive problems within the Indian public education system has been low retention rates beyond primary education, with even lower rates for girls.

One of the most pervasive problems within the Indian public education system has been low retention rates beyond primary education, with even lower rates for girls[34]. In one of the first institutional applications of AI in the social sector in the country, the Government of Andhra Pradesh[35], in partnership with Microsoft, implemented machine learning and analytics through its Azure cloud platform to predict and prevent public school drop-outs. This report aims to use this partnership as a case study to throw into sharp relief the contextual parameters and questions that must be taken into account when evaluating institutional applications of AI in society and developing ethical governance frameworks that can answer to contextual nuances of the application taking cognisance of the actual incidence of its impact. It might also help highlight issues that would be helpful for future deployments in the sector to address, given that the NITI Aayog plans to scale up this project with Microsoft on the basis of the Andhra Pradesh experience[36].

Identifying parameters of algorithmic decision making and its implications for justice and inclusion

Literacy levels in Andhra Pradesh have been the second lowest in the country, with one of the highest percentages of school drop-outs, most of whom come from farming families or those involved in agriculture[37]. It also topped the list of the highest number of female school drop-outs, with seven out of 10 girls dropping out of school before they reach the 10th standard[38]. In a partnership with the Government of Andhra Pradesh, Microsoft offered its Azure cloud computing platform with machine-learning and analytics capabilities as a part of the overall Cortana Analytics Suite (CAS)[39] to develop a predictive model for identifying school drop-outs in the state. The project commenced with a pilot of a little over 1,000 schools and 50,000 students and has now been rolled out to all 13 districts covering 10,000 schools and five million children. The aim of the project was for the information gathered and analysed to be made available to district education officers and school principals who could then deploy targeted interventions and customised counselling[40].

Data was triangulated from three databases in order to build the data pipeline for the project. This included the Unified District Information



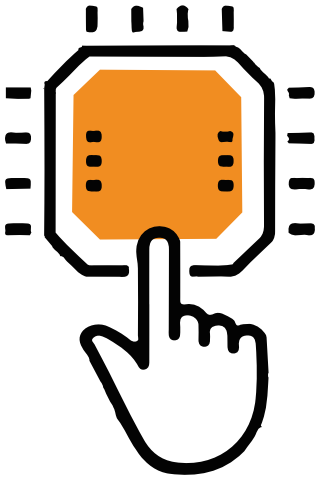
[34]Taneja, A. (2018). The high drop out rates of girls in India. Live Mint. https://www.livemint.com/Opinion/ iXWvKng7uU4L8vo5XbDn9I/The-high-dropout-rate-of-girls-in- India.html [16 Feb 2020].
[35]Andhra Pradesh is a state in south India.
[36]Agha, E., & Gunjan, R. K. (2018). NITI Aayog, Microsoft Partner Up to Predict School Dropouts Using Artificial Intelligence. News18. https://www.news18.com/news/india/niti-aayog- microsoft-partner-up-to-predict-school-dropouts-via-artificial- intelligence-1732251.html [16 Feb 2020].
[37]India Today. (2016). Education survey shows the poor state of Telengana, Andhra Pradesh. India Today. Retrieved from https://www.indiatoday.in/education-today/news/story/ andhra-pradesh-education-319526-2016-04-23 [16 Feb 2020].
[38]Baseerat, B. (2013). Andhra tops in girl school dropouts: Activists. Times of India. Retrieved from https://timesofindia. indiatimes.com/city/hyderabad/Andhra-tops-in-girl-school- dropouts-Activists/articleshow/23937897.cms [16 Feb 2020].
[39]Cortana Analytics Suite is the fully managed big data and advanced analytics suite.
[40]Srivas, A. (2016). Aadhaar in Andhra: Chandrababu Naidu, Microsoft have a plan for curbing school dropouts. The Wire. Retrieved from https://thewire.in/politics/aadhaar-in-andhra-chandrababu- naidu-microsoft-have-a-plan-for-curbing-school-dropouts [16 Feb 2020].

In a partnership with the Government of Andhra Pradesh, Microsoft offered its Azure cloud computing platform with machine-learning and analytics capabilities as a part of the overall Cortana Analytics Suite (CAS) to develop a predictive model for identifying school drop-outs in the state.

System for Education (U-DISE), containing school infrastructure information and the data on teachers and their work experience, education assessment data from multiple sources, and socioeconomic data from the UIDAI[41] Aadhaar system[42]. By aggregating these multiple data points from different sources, the aim of the project is to track the students' journey through the education system by providing a 360-degree view of students after mapping close to 100 variables. Initial results from the project reaffirmed longstanding notions behind school drop-outs. These include girls being more likely to drop out in the absence of ad- equate toilet facilities, higher drop-out rates among students failing to score well in key subjects like English and mathematics, which reduces their faith in formal education, along with the role of the socioeconomic status of the family and the wider community to which the student belongs[43]. In a study based on the National Family and Health Survey-3, it was found that drop-outs tended to be higher among children belonging to minority Muslim families, scheduled castes and scheduled tribes[44]. Further, children belonging to illiterate parents were four times more likely to drop out than those belonging to literate parents. The possibility of children of non-working parents dropping out is also relatively high[45].

Anil Bhansali, the managing director of Microsoft Research and Development, had told the online news outlet The Wire in 2016 that the CAS suite deployed in the project "can provide a lot of useful insight as long as you pump in the data and the right modelling,"[46] with "right modelling" being the operational phrase. With algorithmic decision making coming to play an increasingly significant role in institutionalising individual and systemic bias and discrimination within social systems, it becomes important to evaluate the processes through which these are pervasively deployed.

Data choices: The pilot project was restricted to students of the 10th standard. This is because, ac- cording to Bhansali, the 10th standard represents one of the few inflexion points when one takes their first standardised tests and after which a reasonable number of students drop out on their way to 11th standard. Another likely reason is that 10th standard results are already online and the education department has access to gender and subject grading data through examination hall tickets[47]. Educational assessment information for lower classes entails



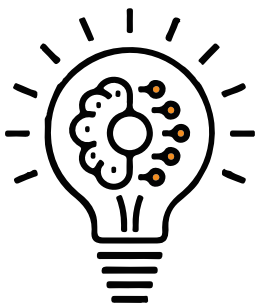
[41]The Unique Identification Authority of India is the entity mandated to issue the 12-digit Aadhaar number and manage the Aadhaar database.
[42]Srivas, A. (2016). Aadhaar in Andhra: Chandrababu Naidu, Microsoft have a plan for curbing school dropouts. The Wire. Retrieved from https://thewire.in/politics/aadhaar-in-andhra-chandrababu- naidu-microsoft-have-a-plan-for-curbing-school-dropouts [16 Feb 2020].
[43]Ibid.
[44]Scheduled Castes and Scheduled Tribes are officially designated historically marginalised groups in India recognised in the Constitution of India.
[45]M., Sateesh, & Sekher, T. V. (2014). Factors leading to school dropouts in India: An analysis of National Family Health Survey-3 data. International Journal of Research & Method in Education, 4(6), 75-83. https:// www.researchgate.net/ publication/269932850_Factors_Leading_to_School_Dropouts_in_India_An_Analysis_of_National_Family_Health_Survey-3_Data [16 Feb 2020].
[46]Srivas, A. (2016). Aadhaar in Andhra: Chandrababu Naidu, Microsoft have a plan for curbing school dropouts. The Wire. Retrieved from https://thewire.in/politics/aadhaar-in-andhra-chandrababu- naidu-microsoft-have-a-plan-for-curbing-school-dropouts [16 Feb 2020].
[47]Examination hall tickets offer rights of admission to a test taker during state or national-level

It is also the case that the drop-out rates are the highest in secondary education (standards 9 and 10),48 coinciding with the completion of standard 8 after which midday meals are no longer provided, which are a major factor driving school attendance.

the herculean task of having to be digitised in order to be of use in a machine-learning system.

However, it is also the case that the drop-out rates are the highest in secondary education (standards 9 and 10),[48] coinciding with the completion of standard 8 after which midday meals are no longer provided, which are a major factor driving school attendance[49]. Those who continue beyond standard 8 to reach standard 10 show a comparative degree of resilience to the non-provision of these sorts of interventions aimed at ameliorating the disadvantageous socioeconomic conditions behind school drop-outs. Therefore, using such data as a training model for the system misplaces the inflexion point and thereby undermines other structural and inter-sectional socioeconomic issues driving high rates of school drop-outs during the transition to secondary education from standard 8 to standard 9. This leads to elision of the structural socioeconomic parameters that constrain equitable access to resources. In addition, the U-DISE database containing information about teachers' work experience does not necessarily map the effectiveness or efficacy of a given teacher and their contribution to better learning outcomes well.

Modelling and inferences: Data choices are not the only criteria determining the questions on inclusion and justice. Decision making regarding the input processes that develop the statistical models and inferences made are equally significant in determining the incidences of impact that a given machine-learning project is likely to have in the areas of its intervention[50]. Given the lack of transparency on the decision-making process, the insights gained from news reports on the subject show that the input process in developing the model involved a combination of existing knowledge, beliefs, and findings about the factors driving school drop-outs, coupled with the convenience of digitised data[51]. Since the extent to which these data were interpreted with bias during the input process is unclear, the extent to which biased socioeconomic profiles based on caste, gender and religion played a role in determining the drop-out rate, versus structural and institutional barriers, is also unclear. Moreover, it is not unlikely that such models can then influence seat allocations within higher education and government services based on such profiles, undermining India's constitution- ally guaranteed affirmative action protections for marginalised and vulnerable groups.



examinations. They contain details of the student like the identity number assigned to the student for the examination, a photograph and a signature along with details of the examination such as location and room (where applicable). Sometimes they also contain the student's name and date of birth. There is no standard format for examination hall tickets and they differ from examination to examination.

[48]PRS Legislative Research. (2017). Trends in school enrolment and drop-out levels. Live Mint. https://www.livemint. com/Education/k1ANVHwheaCFWCupY3jkFP/Trends-in-school- enrolment-and-dropout-levels.html [16 Feb 2020].

[49]Jayaraman, R., Simroth, D., & de Vericourt, F. (n.d.). The Impact of School Lunches on Primary School Enrollment: Evidence from India's Midday Meal Scheme. Indian Statistical Institute, Delhi Centre. Retrieved from www.isid.ac.in/~pu/conference/dec_10_conf/Papers/ RajiJayaraman.pdf [16 Feb 2020]

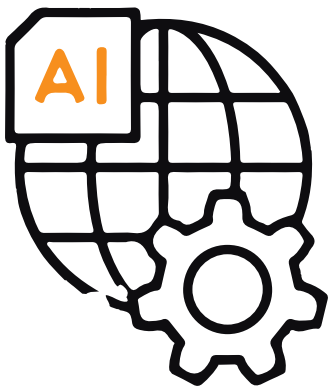
[50]Algorithm Watch. (2019). 'Trustworthy AI' is not an appropriate framework. Retrieved from https://algorithmwatch.org/en/ trustworthy-ai-is-not-an-appropriate-framework [16 Feb 2020].

[51]Srivas, A. (2016). Aadhaar in Andhra: Chandrababu Naidu, Microsoft have a plan for curbing school dropouts. The Wire. Retrieved from https://thewire.in/politics/aadhaar-in-andhra-chandrababu- naidu-microsoft-have-a-plan-for-curbing-school-dropouts [16 Feb 2020].

The movement and replication of data increases the attack surface. These fears are not allayed given that Microsoft is the second most targeted entity after the Pentagon56, and Andhra Pradesh leads in the leakages of sensitive personal data of its constituents.

This highlights the problem of using exist- ing knowledge and statistics in an ahistorical and acontextual manner without duly quantifying the structural and institutional indicators that produce such inequalities in the first place. For example, if the model shows that a Scheduled Tribe girl from Jharkhand is more likely to drop out of school in the absence of a targeted intervention, could this lead to fewer seats allocated in higher education, and reservations in government services for women from the community? Moreover, coupled with data choices, it is unclear to what extent the data trained on standard 10 would be effective in predicting drop-out rates in the transition phase from upper primary (standard 8) to secondary school (standards 9 and 10) where arguably the driving factors are more structural and institutional as compared to performance in a given set of subjects.

Service agreements and data protection: Data sharing within PPPs is unclear due to a lack of transparency, especially in a country like India, which is yet to have its own data protection law but harbours high aspirations of becoming the world leader in AI adoption, deployment and innovation[52]. Bhansali has said that the data is stored in data centres located in India and is tied to the Andhra Pradesh government's account, and that Microsoft cannot own it or repurpose it[53]. own or repurpose the data, it is unclear whether it does or does not have the same rights over the insights generated out of processing of such data. It is also not clear what bespoke – or customised – data protection safeguards were incorporated, if at all, within the public-private agreements. An evaluation study of Microsoft's cloud computing shows that irrespective of the geographical location that a customer selects to locate their data, Micro- soft warns that customers' data, including personal data, may be backed up in the United States (US) by default. Moreover, if any beta or pre-release Microsoft software was used or there was back-up of web or worker role software[54] in any of its cloud ser- vices, data would be stored or replicated in the US[55]. The movement and replication of data increases the attack surface. These fears are not allayed given that Microsoft is the second most targeted entity after the Pentagon[56], and Andhra Pradesh leads in the leakages of sensitive personal data of its constituents[57].



[52]NITI Aayog. (2018). National Strategy for Artificial Intelligence. New Delhi: NITI Aayog. https:// niti.gov.in/writereaddata/files/document_ publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
[53]Srivas, A. (2016). Aadhaar in Andhra: Chandrababu Naidu, Microsoft have a plan for curbing school dropouts. The Wire. Retrieved from https://thewire.in/politics/aadhaar-in-andhra-chandrababu- naidu-microsoft-have-a-plan-for-curbing-school-dropouts [16 Feb 2020].
[54]Web Role is a Cloud Service role in Azure that is configured and customized to run web applications developed on programming languages/technologies that are supported by Internet Information Services (IIS), such as ASP.NET, PHP, Windows Communication Foundation and Fast CGI. Worker Role is any role in Azure that runs applications and services level tasks, which generally do not require IIS. In Worker Roles, IIS is not installed by default. They are mainly used to perform supporting background processes along with Web Roles and do tasks such as automatically compressing uploaded images, run scripts when something changes in the database, get new messages from queue and process and more." Source: https:// cloudmonix.com/blog/what-is-web-and-worker-role-in-microsoft-azure.

[55]Calligo. (n.d.). Microsoft Azure and Data Privacy. Retrieved from https://calligo. cloud/ wp-content/uploads/Azure-Data-Privacy-Stack.pdf?utm_ campaign=Hybrid%20Azure&utm_ source=hs_automation&utm_ medium=email&utm_content=69182393&_hsenc=p2ANqtz-8e2YnyrNnNj0uMWxrv8oaYaLLlso_vi8apwlbq3HTVVRqgl2WY94jmA KBStWuDTwC-U1F_ NPubB4SltezcA43mZl1YTw&_hsmi=69182393 [16 Feb 2020].
[56]Ibid.
[57]See, for example: MediaNama. (2019). Andhra Pradesh exposes Aadhaar of farmers - once again. MediaNama. Retrieved from https://www. medianama.com/2019/05/223-andhra-pradesh-exposes-

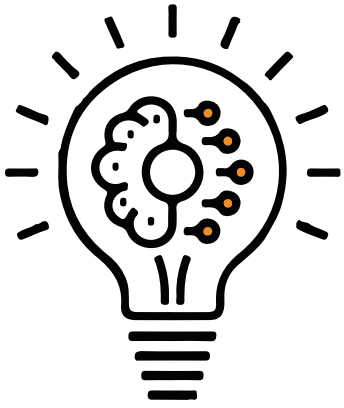
Significant international multilateral and multi-stakeholder attention has been diverted towards developing ethical governance frameworks for AI.

Conclusion

Given that AI systems are increasingly aiding state institutions in the allocation of resources, it becomes imperative that they align with principles of non-discrimination rather than perpetuate existing misallocations by creating pervasive systems of privilege being trained on unrepresentative data sets and models. Significant international multilateral and multi-stakeholder attention has been diverted towards developing ethical governance frameworks for AI. This includes the OECD Principles on AI[58], the European Commission Ethical Guidelines for Trustworthy AI[59], as well as the Toronto Declaration: Protecting the Right to Equality and Non-Discrimination in Machine Learning Systems[60], along with attention in other digital policy global initiatives like the United Nations High-Level Panel on Digital Cooperation.

However, these provide broad-based principles without adequately applied examples, which delimit their uptake and applicability and serve to act as an "alternative or preamble to regulation", there- by diluting "state accountability and rights-based obligations."[61] These also serve to act as light- touch non-discrimination norms that provide the leeway for businesses to not actually engage with non-discrimination principles within data choices, modelling, design and application, thereby ending up entrenching discrimination by making inequalities institutionally pervasive. A second approach, which is a technical approach, aims to ensure fairness, accountability and transparency (FAT) in AI systems. However, the FAT approach fails to identify structural socioeconomic indicators to contextualise the principles of non-discrimination within systems design[62].

It has been argued that multilateral commitments to universally agreed human rights principles with regard to AI would serve to strengthen the intended application of both these approaches[63]. However, all approaches must be accompanied with evidence-based case studies to develop principled processes like algorithm impact assessments, explainability, transparency of commercial contracts, etc. with a clear understanding of learnings from use cases, and the role of different



aadhaar-of- farmers-once-again [16 Feb 2020]; Jalan, T. (2018). CCE-Andhra Pradesh leaks students' gender, caste, quota, Aadhaar data on website. MediaNama. Retrieved from https://www.medianama.com/2018/08/223-apcce- students-aadhaar-exposed [16 Feb 2020]; Tutika, K. (2018). Aadhaar data leak of Andhra Pradesh women raises security concerns. The New Indian Express. Retrieved from www.newindianexpress.com/states/andhra- pradesh/2018/mar/20/aadhaar-data-leak-of-andhra-pradesh-women-raises-security-concerns-1789648.html [16 Feb 2020].

[58]OCED. (2019). OECD principles on AI. Retrieved from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [16 Feb 2020].

[59]Independent High Level Group on Artificial Intelligence. (2018). Ethics guidelines for trustworthy AI. European Commission. Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation [16 Feb 2020]

[60]The Toronto Declaration. (2018). The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems. Access Now. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf [16 Feb 2020].

[61]ARTICLE 19. (2019). Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence. London: ARTICLE 19. Retrieved from https://www.article19.org/wp-content/ uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf [16 Feb 2020]

[62]Ibid.

[63]Ibid.

stakeholders within the process, rather than principled outcomes like trustworthy AI and fair and ethical machine-learning systems.

Action steps

The following advocacy steps are suggested for India:

- *Risk sandboxing*: Regulatory sandboxing[64] and data sandboxing[65] are often recommended tools that create a facilitative environment through relaxed regulations and anonymised data to allow innovations to evolve and emerge. How- ever, there also needs to be a concomitant risk sandboxing that allows emerging innovations to evaluate the unintended consequences of their deployment. Risk sandboxing is envisaged as a natural progression from regulatory sandboxing in which the product is tested for its decision-making impact on vulnerable and marginalised populations on the basis of non-discrimination principles.
- *First stage process-based transparency*: While there has been much discussion about the need for explainable AI to counter the black-boxing phenomenon underlying AI's opaque decision-making process, there needs to be a first-level transparency with respect to the inputs into the model development process, data choices, and platform capabilities and jurisdictions.
- *Disclosure of service agreements:* There need to be disclosure of service agreements within PPPs deploying AI technologies to understand the data protection commitments and data-sharing practices.
- *Mapping contextual parameters of knowledge used in modelling:* Studies that constitute knowledge about a given subject area are the result of divergent research objectives which should be evaluated for their relevance and bearing to the machine-learning system being deployed before they are factored into predictive modelling. Moreover, socioeconomic and structural indicators – such as caste, gender and family income in conjunction with how that caste group fares overall in the economy – must be identified and mapped into the model along with transparency on the decision making that maps these indicators to train the machine learning system.

[64] Regulatory sandboxing allows for a controlled environment with relaxed regulations that allows a product or innovation to be thoroughly tested out before being released for public use. It involves a set of rules that allow innovators to test their products within a limited legal environment subject to pre- defined restrictions like limitation on exposure, time-limited testing, pre-defined exemptions, and testing under regulatory supervision. Source: https://cis-india.org/internet-governance/ files/ai-in-india-a-policy-agenda/view; pubdocs.worldbank.org/ en/770171476811898530/Session-4-Pavel-Shoust-Regulatory- Sandboxes-21-09-2016.pdf

[65] Data sandboxes allow companies to access large anonymised data sets under controlled circumstances to enable them to test their products and innovations while keeping in mind privacy and security compliance requirements.

- *Representative data choices:* The data on which a machine-learning system is trained must be representative of the population in which it is to be deployed.
- *Recommendations structured on non-discrimination principles:* Recommendations must be structured on non-discrimination principles. This should be done, for example, to avoid in- stances when an AI system recommends fewer STEM (science, technology, engineering and mathematics) courses for women because the data shows women are less likely to take up STEM subjects.

Building Data Architectures for AI (Artificial Intelligence) Driven Efficiency in **Healthcare**

Identity, Ownership, And Privacy

BUILDING DATA ARCHITECTURES FOR AI DRIVEN EFFICIENCY IN HEALTHCARE: IDENTITY, OWNERSHIP, AND PRIVACY

Addressing institutional and capacity gaps in healthcare

Artificial Intelligence (AI) in the healthcare market is set to grow at a rate of 40% by 2021 which could help bridge India's poor doctor-patient ratio[66]. In 2019 India had 1 government doctor per 10,189 persons in the population while the recommended limit by the World Health Organisation is 1:1000[67]. It currently has a shortage of 600,000 doctors and 2 million nurses. This underscores the institutional and infrastructural gaps plaguing India's healthcare sector where private healthcare expenditure stands at around 70% with 62.4% out of pocket expenses[68] pushing people into poverty. Moreover, 67% of the doctors and 70%[69] of the country's healthcare infrastructure is present in the urban areas while 66% of the population resides in the rural areas[70]. Thus the lack of qualified medical professional, non-uniform access to healthcare across the country, and affordability compound the access to quality healthcare for large sections of the Indian populations who are marginalised and underserved thereby stalling their ability to improve their livelihoods. It is expected that the adoption of emerging technologies like AI will enable India to leverage its limited resources, infrastructures, and institutions to increase healthcare coverage with a bonus move towards preventive healthcare through early detection. It is expected to maximise the volume of patients served by physicians by automating the physical screening of samples by highlighting the samples that require their expertise.

Trends in AI adoption

The adoption of AI in healthcare in India is increasing at an increasing pace where developers partner with hospitals towards pilot and application of related technologies. 31% of the global executives interviewed about the most disruptive technologies in healthcare reported such technology to be AI while 42% Indian executives reported to be investing in AI for healthcare[71]. Given the diversity of the healthcare ecosystem, the applications of AI in different sub-sectors

[66] Business Wire. (2019). Artificial Intelligence (AI) in Healthcare Market in India is Expected to Grow at a Rate of 40% by 2021, Impacting the Doctor-Patient Ratio During the Forecast Period, 2018-2023. Retrieved from https://www.businesswire.com/news/home/20190726005157/en/Artificial-Intelligence-AI-Healthcare-Market-India-Expected [18 Feb 2020].

[67] Press Trust India. (2019). India facing shortage of 600,000 doctors, 2 million nurses: Study. Economic Times. Retrieved from https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/india-facing-shortage-of-600000-doctors-2-million-nurses-study/articleshow/68875822.cms?from=mdr [18 Feb 2020].

[68] PricewaterhouseCoopers. (2018). Reimagining the possible in the Indian healthcare ecosystem with emerging technologies. Bengal Chambers of Commerce and Industry and PricewaterhouseCoopers. Retrieved from https://www.pwc.in/assets/pdfs/publications/2018/reimagining-the-possible-in-the-indian-healthcare-ecosystem-with-emerging-technologies.pdf [16 Feb 2020].

[69] Business Wire. (2019). Artificial Intelligence (AI) in Healthcare Market in India is Expected to Grow at a Rate of 40% by 2021, Impacting the Doctor-Patient Ratio During the Forecast Period, 2018-2023. Retrieved from https://www.businesswire.com/news/home/20190726005157/en/Artificial-Intelligence-AI-Healthcare-Market-India-Expected [18 Feb 2020].

[70] PricewaterhouseCoopers. (2018). Reimagining the possible in the Indian healthcare ecosystem with emerging technologies. Bengal Chambers of Commerce and Industry and PricewaterhouseCoopers. Retrieved from https://www.pwc.in/assets/pdfs/publications/2018/reimagining-the-possible-in-the-indian-healthcare-ecosystem-with-emerging-technologies.pdf [16 Feb 2020].

[71] Ibid.

The lack of qualified medical professional, non-uniform access to healthcare across the country, and affordability compound the access to quality healthcare for large sections of the Indian populations who are marginalised and underserved thereby stalling their ability to improve their livelihoods.

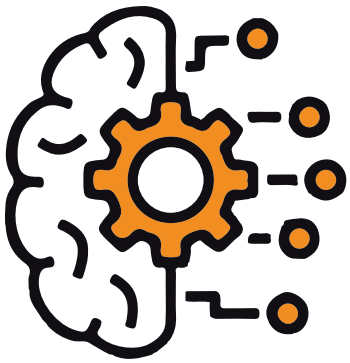
differ as per the requirements. In line with their outputs, the types of AI applications could be divided into three broad categories: descriptive, predictive, and prescriptive.

Descriptive application of AI relates to events that have already occurred and in order detect minor changes and trends in such events that might escape human detection like detecting subtle fractures and skin lesions. Predictive applications relate to data about events that have already occurred in order to provide predictions for the future that can help in preventive disease identification and by upstreaming critical cases to physicians with the effect of cutting down on manual screening. Prescriptive statistics go one further from predictive statistics to suggest potential treatments with changes in diagnosis[72].

AI application in the healthcare sector in India can be divided into two major trends: (1) through home grown start-ups driving website/ app based and business solutions; and (2) through partnerships by global technology companies with private hospitals and clinical establishments. Through the former mode, AI applications in healthcare are based around image parsing algorithms towards prediction/ detection of cancer, tuberculosis and acute infections, retinal analysis and diabetic retinopathy, and malignancy scoring and surgical planning. Apart from this AI has been deployed to predict diseases like cancer, diabetes, neurological disorder, and cardiovascular diseases from genomic data; provide business solutions in AI for insurance, health, and Fintech; and use AI powered medical data to test blood, urine, sperm apart from retinal scanning and x-ray.

Through the latter mode (i.e. through partnerships by global technology companies) IBM Watson for Oncology has tied up with Manipal Group of Hospitals for diagnosis and treatment of 7 types of cancers. Arvind Eye Care is working with Google Brain for detecting diabetic retinopathy where Arvind Eye Care has provided Google with images to train it algorithm which is now being used to put to routine use with its patients. Microsoft's Azure Cloud Computing, Machine Learning, Data Analytics, CRM online and Office 365 are used by private healthcare providers like Fortis Healthcare, Apollo Hospitals, L V Prasad Eye Institute, Narayana Health, and Max Healthcare.

Different government initiatives have highlighted the policy intent to mainstream AI within healthcare through budget allocations and PPPs. The Karnataka Government is planning to mobilise INR 2000 crore in order to support AI start-ups. The Karnataka Government also has a start-up policy and Karnataka Information Technology Venture Capital Fund that can support start-ups[73]. The year 2020 has been declared as the year of AI by the Telangana Government as a result of agreements signed with several companies as well as with the premier



[72] Paul, Y., Hickok, E., Sinha, A., & Tiwari, U. (2018). Artificial intelligence in the healthcare industry in India. Centre for Internet and Society. Retrieved from https://cis-india.org/internet-governance/files/ai-and-healtchare-report [25 Feb 2020]

[73] MedicalBuyer. (2019). Indian Healthcare Is All Set To Be Transformed By AI. Retrieved from https://www.medicalbuyer.co.in/indian-healthcare-is-all-set-to-be-transformed-by-ai/ [25 Feb 2020].

31% of the global executives interviewed about the most disruptive technologies in healthcare reported such technology to be AI while 42% Indian executives reported to be investing in AI for healthcare.

Indian Institute of Technology (IIT), Kharagpur for development in Telangana[74]. Through this initiative the state government aims to leverage the data of 40 million of its citizens through technology such as AI and machine learning. The state also aims to use deep technology to transform public service delivery and governance[75].

The Prime Minister's Office has signed a pact with the Israeli government that put in place a tie-up between Bengaluru-based Telerad Tech (an affiliate of Teleradiology Solutions) and Israel-based Zebra Medical Vision to use AI in radiology in order to allow auto and intelligent detection of cancer, stroke, fractures and other medical conditions[76]. NITI Aayog has partnered with Microsoft to build AI assisted models for screening diabetic retinopathy to support early risk detection, risk assessment, and timely medical intervention. These models will be deployed as proofs of concept across Primary Health Centres identified by NITI Aayog. Microsoft will also help NITI Aayog develop a blueprint for AI-led diabetic retinopathy programmes which can be used by Central and State governments to incorporate into their respective health screening and programmes[77].

Creating data architectures for integrating AI in healthcare

In cognizance of the deepening integration of emerging technology and big data analytics in healthcare systems there have been regulatory developments and policy initiatives in this area. In its paper on moving towards 21st century healthcare, NITI Aayog has highlighted the importance of digital health or a digital ecosystem of healthcare. Underlying the regulatory initiatives and policy proposals were the move towards developing and maintaining a national level integrated information ecosystem with the aim of increasing access, efficiency, cost-effectiveness, and equity in the provision of health services[78]. Some of the challenges identified by the NITI Aayog in moving towards an ecosystem of healthcare information ecosystem involve the need to identify each patient with a unique ID through their Aadhaar card, having computer coded registries of data from healthcare service providers, the need to have a fully functioning integrated ecosystem

[74] Venkatest, H. (2020). 2020 Declared Year of Artificial Intelligence in Telangana as Govt Signs MoUs with Cos, IITs. News18. Retrieved from https://www.news18.com/news/india/2020-declared-year-of-artificial-intelligence-in-telangana-as-govt-signs-mous-with-cos-iits-2443623.html [25 Feb 2020]

[75] Lasania, Y. (2020). Telangana government launches AI projects, ties up with tech firms. LiveMint. Retrieved from https://www.livemint.com/technology/tech-news/telangana-declares-2020-as-year-of-ai-launches-series-of-projects-11577968436942.html [25 Feb 2020]

[76] Rao, S. R. (2017). Bengaluru, Israeli firms join hands to deploy artificial intelligence. Time of India. Retrieved from https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-israeli-firms-join-hands-to-deploy-artificial-intelligence/articleshow/59485190.cms [25 Feb 2020].

[77] Microsoft New Centre India. (2018). NITI Aayog forges agreement with Microsoft India to bring the power of AI to the masses. Retrieved from https://news.microsoft.com/en-in/niti-aayog-microsoft-india-ai-agreement/ [25 Feb 2020]

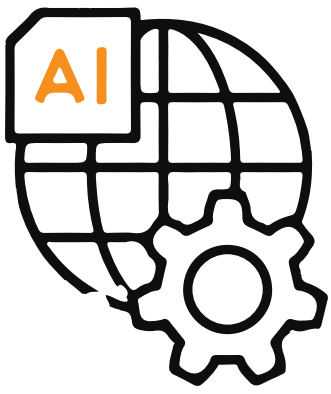
[78] NITI Aayog. (2019). Health system for a new India: Building blocks. Retrieved from https://niti.gov.in/sites/default/files/2019-11/NitiAayogBook_compressed.pdf

With AI being a general purpose technology these specification and legal prescriptions have to contend with sectoral policies as well as the regulation of the technical infrastructure itself which has a potential impact of leaving risk interfaces and regulatory blindspots that can widen the scope of violations of privacy

of digital health data, the lack of prominent health IT vendors and entrepreneurs, and lack of information standards.

One of overarching recommendations across health and digital policy is of the National Health Stack (NHS) which will facilitate the collection of comprehensive health data across the country with the purported aim of smart policy-making and any research and innovation by other stakeholders who can build over these blocks. The National Health Stack is premised on the Aadhaar unique identification system to develop a unique identifier in the nature of a Digital Health ID based upon a more foundational national ID/ identifier like the Aadhaar on the production of which an individual would be entered into the system of registered beneficiaries as a part of the National Health Resource Registry. The National Health Stack (NHS) is envisaged as being built on the backbone of a number of national level databases like the National Health Resource Registry mentioned above, claims and coverage platform, personal health records, national health analytics platform. The aim of the NHS is to work as a presenceless, paperless, cashless consent layer.

However, the aspirations towards an NHS lacks digitized health data required for the purpose. In order to take a positive direction in this space, the government has come up with policy initiatives in this area to formalize the process that establishes the layer of digitized health data. The primary document in this respect is the National Health Policy, 2017 which proposes a National Health Information Architecture, Health Information Exchanges, and National Health Information Network by 2025. Although the Clinical Establishment (Central Government) Rules, 2012 was an early step towards digitisation of health records it never transformed into a national level system. The 2017 Policy includes proposition for a federated national health information system, linking public and private health systems at state and national levels consistent with Metadata and Data Standards and Electronic Health Record, using Aadhaar as the unique identifier, creation of registries (of patients, diseases, service providers etc.) for enhanced public health and big data analytics, and use of Fibre Optic Network and smartphones and tablets for capturing real time data. However, the digitisation of health data is not only towards the delivery of healthcare services but also towards supporting and delivering the criminal justice system through the DNA Technology (Use and Application) Regulation Bill, 2018 which aims to be a National, Regional, State DNA Bank for the purposes of establishing the identity of certain categories of persons including victims, offenders, missing persons, unidentified bodies etc[79]. However, India's AI aspirations in healthcare have to contend with technical limitation and policy intent and effect working at cross-purposes.



[79]Jalan, T. (2018). Union cabinet approved DNA profiling bill. Medianama. Retrieved from https://www.medianama.com/2018/07/223-union-cabinet-approves-dna-profiling-bill/ [25 Feb 2020].

Within policy, a digital health ecosystem has emerged as the precursor to institute the fruits of AI driven efficiency within the public service delivery of healthcare.

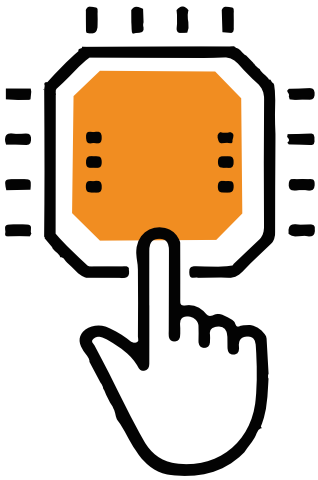
Identity, ownership, and privacy

The implementation of AI in healthcare in India contends with the establishment of a technical architecture and the legal and regulatory framework. With AI being a general purpose technology these specification and legal prescriptions have to contend with sectoral policies as well as the regulation of the technical infrastructure itself which has a potential impact of leaving risk interfaces and regulatory blindspots that can widen the scope of violations of privacy. This is highlighted in the concerns about ownership, identity, data protection, representativeness, surveillance, safety and security.

Identity: The public data architecture on which the AI is said to be premised is predicated on a layer of of unique identifier built presumably on the foundational identifier of the Aadhaar. The Aadhaar database already contains biometric information, bank details, details of tax returns, details of individuals availing social protection[80]. Policy proposition aims to add/integrate the layer of sensitive personal health information on top of this layer in order to create uniquely identifiable health data information infrastructure. Given the security breaches reported with the Aadhaar database, this heightens the risk interface given the sensitive nature of health data. Where the JAM trinity and IndiaStack form the basis of the National Health Stack and underpins the data framework and architecture on which the digital transformation of the healthcare system is premised it inherits the vulnerabilities of the foundational layer and exacerbates the fallouts from encroachment on privacy given the sensitive nature of the information stored.

Ownership: The ownership and proposed operational management of health information infrastructure is unclear. However, the Report of the Technical Advisory Group for Unique Projects (TAGUP) provides an indication of how much ecosystems might be managed. According to the TAGUP Report

- under the the Ministry of Finance talks about the creation of National Information Utilities (NIUs) to manage such data present with the government (CIS, 2016). NIUs are described as a 'class of institutions' who would act as a middleman between the government and vendors to handle all aspects of IT projects for complex projects. As per the TAGUP report the NIUs would be made up of private profit-making companies



[80]In 2017, the Central Government in India mandated the linking of Aadhaar with banks accounts and mobile numbers at the suspension of services. The linkage deadline was given to be 31 Dec 2017 with a extension up to 31 March 2018. However, mobile numbers were provided during Aadhaar enrolment in order to receive alerts and one time passwords. However, in March 2018 the Supreme Court ruled that the mandatory linking of Aadhaar to bank accounts and mobile numbers stand suspended indefinitely till judgement is pronounced on petitions before it. Subsequently, in the Aadhaar judgement delivered by the Supreme Court it is not mandatory to link Aadhaar to financial services like bank accounts, mutual funds etc. but it is still mandatory to quote the Aadhaar unique identification number for filing income tax and linking the PAN (Permanent Account Number) Card. The PAN Card is a 10 digit alpha numeric identity allotted to each taxpayer by the Income Tax Department under supervision of the Central Board of Direct Taxes. Aadhaar Card remains mandatory for the provision of state services like social protection. Despite the Supreme Court ruling, a significant number of bank details and mobile numbers were already linked and in practice, service providers insist on Aadhaar as a means of verification.

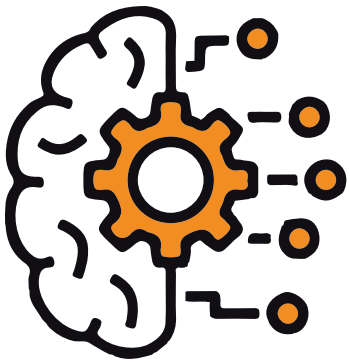
The purpose of a data warehouse is to act as "goldmine of health data (a "data warehouse") to be studied by epidemiologists, other population health specialists, pharmaceutical interests and others with an eye toward innovation and identifying strengths and weaknesses within the health ecosystem".

with very little regulatory oversight and would be completely privately owned with *at least* 51% private ownership (with a 25% cap per entity) and at least 26% government ownership. Though technology companies are barred from being shareholders due to conflicts of interest, deployment of complex corporate structures in order to circumvent such rules is not unheard of[81].

Privacy: NITI Aayog's vision of a digital health ecosystem does not incorporate the considerations under Digital Information Security in Healthcare Act (DISHA) which places narrower purpose limitations with a consent-centred approach at every stage of processing. These leads to a dissonance between policy objectives and legislative provisions. This is particularly germane given the fact that the draft data protection bill is weaker in providing protections with respect to a wide ambit for non-consensual processing where DISHA does not. Though stronger in safeguards compared to the draft data protection bill, DISHA does not address autonomy of the individual with regard to data stored on digital infrastructures developed and deployed by private entities.

Conclusion

Within policy, a digital health ecosystem has emerged as the precursor to institute the fruits of AI driven efficiency within the public service delivery of healthcare. This hinges on 6 critical pillars of an enabling governance regime, interoperability standards of health data dictionary, a three tier framework of building Hospital Information System (HIS), health insurance information system for 'health payers' (insurance companies) in moving towards a system of electronic health records and health data warehouse culminating in the creation of the health information infrastructure. The three tier framework of HIS aims to aggregate data from inventories, referrals, admission and discharge records, out-patient registries etc. (Level 3) through lab orders and results, surgery and appointment schedules, pharmacy orders etc. (Level 2) up to the creation of electronic medical records and clinical decision support (Level 1). Thus, it encompasses the recording and registration of every interface of an individual as a patient seeking medical care. The purpose of a data warehouse is to act as "goldmine of health data (a "data warehouse") to be studied by epidemiologists, other population health specialists, pharmaceutical interests and others with an eye toward innovation and identifying strengths and weaknesses within the health ecosystem" (p. 256). The aggregation of sensitive personal data like health data without purpose limitation, the integration of the same with an insurance ecosystem, combination of data with undefined access underscores the shaky foundations of data governance and inadequate safeguards on which the deployment of pervasive technologies like AI are predicated. Given the significant risk of harms current propositions

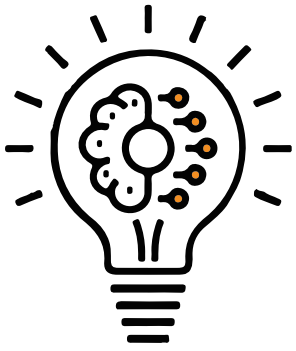


[81] Nandi, A. (2019). India's fast approaching data driven anti-trust reckoning. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536118 [25 Feb 2020].

have with regarding infringement of privacy with regard to sensitive personal health data, it becomes imperative to move towards its operational practice with due consideration for safeguards.

Recommendations

- **Harmonisation of policies**: Given contending provisions, attendant gaps, and divergent incidence of impact across the National Health Policy, Digital Information Security in Healthcare Act (DISHA), the draft data protection bill, and DNA Regulation bill it becomes imperative to undertake an exercise towards harmonising the provisions and objectives of different legislation and proliferating policy exercise to prevent them from act at cross-purposes with each other.
- **Delineating ownership**: Given the development of the technical infrastructures for hosting the digital health ecosystem will be done by private companies, it becomes important to delineate ownership and storage of data along with standards and conditions for operational management.
- **Separate health service delivery and criminal justice**: It is important to prevent the possibility of functional creep between the storage of health data for public health service delivery and storage of DNA data for criminal justice purposes.
- **Establish purpose limitation**: Given the scale of proposed data collection, it becomes important to narrowly delineate the purposes for electronic data at point of health service delivery could be aggregated and combined.
- **Establish access protocols**: With the proposed move towards creation of a data warehouse it becomes important to specify access protocols, particularly in the absence of prescribed anonymisation standards. For example, only authorised professionals can have access by sanction from relevant authority in case of public health emergencies. Though DISHA appear to place The National Electronic Health Authority as the gatekeeper, the propositions and roadmap put forward by NITI Aayog take limited cognisance of it.



- **Isolate insurance platform from electronic health records**: Isolating insurance platforms from electronic health data platforms are integral to prevent misuse of the system towards discriminatory pricing.
- **Align policy and legislative provisions**: Given the divergence between policy intent, objectives and propositions for a national health architecture and given legislative provisions, it becomes important to align them in order promote greater transparency of operations.

Automated decision-making systems in **law enforcement**

On the need to balance between privacy and security

AUTOMATED DECISION-MAKING SYSTEMS IN LAW ENFORCEMENT: ON THE NEED TO BALANCE BETWEEN PRIVACY AND SECURITY

Prevalence of AI use in law enforcement: Nature and types of application

AI in law enforcement has been with the purpose of augmenting policing and law enforcement capabilities. This has been in the area of predictive policing, apprehending criminal offenders, early detection, and reducing time lag in information available to front line responders. Despite the NITI Aayog Strategy paper highlighting the importance of AI in social sector applications like healthcare, agriculture, education, smart cities and infrastructure, and smart mobility and transportation AI use cases in law enforcement are significantly higher than individual social sector applications[82]. Further, contrary to the trend in other sectors AI in law enforcement have domestic companies as the leading player in the domain as opposed to international ones, with STAQU currently leading the fray in developing proprietary algorithms for law enforcement though NEC Corporation had the first mover advantage by developing the first real time facial recognition system for the Surat Police (Gujarat) in 2015. Three key areas that can be broadly identified include (i) predictive policing; (ii) facial recognition; and (iii) Crime and Criminal Tracking Network and Systems (CCTNS). Close to 50% of Indian states are already using or planning to use AI in law enforcement - these include the states of Rajasthan, Maharashtra, Delhi, Jharkhand, Punjab, West Bengal, Telangana, Assam[83], Haryana, Uttarakhand, Tamil Nadu, Uttar Pradesh, Odisha, Kerala, Gujarat[84], and Andhra Pradesh. Apart from these other users include National Crime Records Bureau (NCRB), Railway Protection Force, and Ministry of Women and Child Development.

State Profiles

Rajasthan

In 2017, the district police of Alwar in Rajasthan commissioned a pilot project with STAQU called ABHED (Artificial Intelligence Based Human Efface Detection). ABHED is STAQU's proprietary technology stack delivered through an app with a simplified user interface that allows police personnel to have real time information for criminal identification through biometric identification with fingerprint, voice, and facial recognition with the potential for being integrated with CCTNS and use for tracking missing persons. ABHED can profile criminals or missing persons and also be used for criminal registration. It is optimised for 2G and 3G networks with login and password for each police personnel with access that can be controlled through OTP based logins at various levels with mobile phones. It can retrieve

[82] see Basu, A. & Hickok, E. (2018). Artificial intelligence in the governance sector in India. Centre for Internet and Society. Retrieved from https://cis-india.org/internet-governance/ai-and-governance-case-study-pdf [16 Feb 2020].

[83] Sengupta. A. (2019). Artificial intelligence to create smart cops in Assam. The Telegraph. Retrieved from https://www.telegraphindia.com/states/north-east/artificial-intelligence-to-create-smart-cops-in-assam/cid/1684018 [15 Feb 2020]

[84] Mehta, Y.B. (2015). In a first, real time facial recognition system launched by Surat Police. The Times of India City. Retrieved from https://timesofindia.indiatimes.com/city/surat/In-a-first-real-time-facial-recognition-system-launched-by-Surat-police/articleshow/48135306.cms [15 Feb 2020].

Despite the NITI Aayog Strategy paper highlighting the importance of AI in social sector applications like healthcare, agriculture, education, smart cities and infrastructure, and smart mobility and transportation AI use cases in law enforcement are significantly higher than individual social sector applications.

information from criminal databases in real time and can perform search through FIR, available face images, and fingerprints[85]. The company boasts greater accuracy than other criminal recognition platforms at 95%[86]. STAQU used its learning's from the Rajasthan pilot to develop the Punjab Artificial Intelligence System (PAIS) and is currently exporting ABHED to Dubai Police to help in crime reduction by 25%[87].

Punjab

PAIS earned the FICCI (Federation of Indian Chambers of Commerce and Industry) Smart Policing Awards in 2018. With PAIS, STAQU started with the basic step of digitising all records that helped automate criminal search along with other critical analysis required by police personnel in operational processes[88]. PAIS used advance facial recognition with natural language processing, gang analysis and phonetic search technologies to provide a unified and integrated provision of service[89]. STAQU has now trademarked PAIS as the Police Artificial Intelligence System claimed to be the 'Ultimate Digital Dossier' for police personnel in investigation and criminal apprehensions[90]. In 2019, the Punjab Police was again the recipient of FICCI Smart Policing Awards this time for the Punjab Information News Extractor (PINE) for the gathering of Open Source Intelligence that aggregated data from different sources and data types in order to process such information and extract relevant attributes for delivering to the stakeholders involved. It also has the capability to extract information from breaking news on TV channels on pre-defined topics in order to develop alert and information retrieval, if required[91]. PINE, too, is currently trademarked by STAQU[92].

Delhi

Delhi Police, as per its Vision 2020, aimed to adopt technology based policing using artificial intelligence and big data that will revolve around predictive policing, connected multi-jurisdictional records, connecting multi-jurisdictional records, integrating human intelligence as the centre-piece, centralised database for remote suspect verification with a seamless and integrated platform for service delivery[93]. Delhi Police

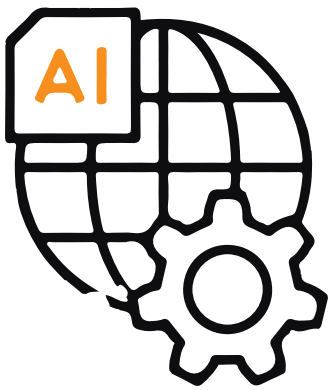
[85] IANS. (2017). Alwar police is using an AI programme to register criminal offences. Tech2. Retrieved from https://www.firstpost.com/tech/news-analysis/alwar-police-is-using-an-ai-programme-to-register-criminal-offences-3703601.html [14 Feb 2020].
[86] Mullick, S. (2018). This AI startup has created a minority report like AI policing system. Digit. Retrieved from https://www.digit.in/features/machine-learning-and-ai/gurugram-based-staqu-has-developed-a-minority-report-like-ai-smart-policing-system-42154.html [14 Feb 2020].
[87] Pandit, V. (2018). Dubai police ties up with Indian start-up on AI based solution for predictive policing. The Hindu Business Line. Retrieved from https://www.thehindubusinessline.com/info-tech/dubai-police-ties-up-with-indian-startup-for-ai-based-solution-on-predictive-policing/article24318442.ece [14 Feb 2020].
[88] Ujaley, M. (2018). Punjab Police won smart policing award for Punjab Artificial Intelligence System. Express Computer. Retrieved from https://www.expresscomputer.in/egov-watch/punjab-police-won-smart-policing-award-for-punjab-artificial-intelligence-system/24958/ [14 Feb 2020].
[89] FICCI. (2018). Winners of the FICCI Smart Policing Awards 2018.
[90] STAQU. (n.d.) PAIS. Retrieved from https://www.staqu.com/pais/ [14 Feb 2020].
[91] FICCI. (2019). Compendium of best practices in smart policing. Smart Policing Awards 2019. Retrieved from http://ficci.in/spdocument/23116/FICCI-Compendium-of-Best-Practices-in-sMART-Policing-2019.pdf [14 Feb 2020].
[92] STAQU. (n.d.). PINE. Retrieved from https://www.staqu.com/pine/ [14 Feb 2020].
[93] IANS. (2017). Delhi Police to adopt 'technology based policing'; use artificial intelligence and data analytics by 2020. Tech2. Retrieved from https://www.firstpost.com/tech/news-analysis/delhi-police-to-

CCTNS by NCRB is a nation-wide networking infrastructure that aims to be a comprehensive database for crimes and criminals, work as a national and state-level database of crime and criminal records, and be a platform for state police to enter details of a crime into the centralised system.

has acquired and integrated facial recognition system with missing and found children/ persons module of the Zonal Integrated Network system (ZIPNET). It will also help in the identification of missing children who are found after a long by being able to account for the ageing process. It further helps in surveillance and detection of children in crowded places like railway station, public rallies, bus terminals among others[94]. In 2016, in partnership with the Indian Space Research Organisation (ISRO) it aimed to deploy Crime Mapping, Analytics and Predictive System (CMAPS)[95] to cluster maps areas by triangulating call data from the city's emergency helpline number 100 and ISRO's satellite imageries to determine crime hot spots to deploy police to such locations for preventive action[96]. The system would be complete with with police officer equipped with Personal Digital Assistants through which they can access criminal databases in real time which stored a record of more than 200,000 criminal in 2016[97]. In 2018, the Indraprastha Institute of Information Technology (IIIT) set up a Centre for Technology and Policing that would help the Delhi Police in using artificial intelligence, big data and network forensics, cyber policing, social media analysis, and biometrics and image processing[98]. The Delhi Police have started using facial recognition technology to monitor political rallies by comparing it against footage of previous protests in the city to identify "alleged 'rabble rousers and miscreants'"[99]. Prior to this it had used facial recognition technology in Republic Day and Independence Day parades to scan footage and match it against its database of known criminal and terrorists[100].

Uttar Pradesh

Leveraging its learning from previous deployments in Rajasthan and Punjab STAQU deployed Trinetra in Uttar Pradesh of an app powered by the company's expertise is biometric identification and using machine learning and deep learning to work well even with low resolution images to facilitate biometric parsing while deploying using gang identification technology to identify not just the criminal but also



adopt-technology-based-policing-will-use-artificial-intelligence-and-data-analytics-by-2020-4180695.html [14 Feb 2020].

[94] Delhi Police. (n.d.) Best practices in Delhi Police. Retrieved from https://www.delhipolice.nic.in/Best_practices.pdf [14 Feb 2020].

[95] Seeraj, TK. (2016). Delhi Police to start 'predictive policing', to use space technology for crime mapping. ScoopWhoop. Retrieved from https://www.scoopwhoop.com/Delhi-Police-To-Start-Predictive-Policing-To-Use-Space-Technology-For-Crime-Mapping/ [14 Feb 2020].

[96] Singh, K.P. (2017). Preventing crime before it happens: How data is helping Delhi Police. Hindustan Times. Retrieved from https://www.hindustantimes.com/delhi/delhi-police-is-using-precrime-data-analysis-to-send-its-men-to-likely-trouble-spots/story-hZcCRyWMVoNSsRhnBNgOHI.html [14 Feb 2020].

[97] Press Trust of India. (2016). Delhi police to use space tech for crime control. Economic Times. Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/delhi-police-to-use-space-tech-for-crime-control/articleshow/50887300.cms [14 Feb 2020]

[98] Press Trust of India. (2018). Delhi police get artificial intelligence centre to fight crime, terrorists. Business Standard. Retrieved from https://www.business-standard.com/article/current-affairs/delhi-police-gets-artificial-intelligence-centre-to-fight-crime-terrorists-118120400449_1.html [14 feb 2020]

[99] Mazoondar, J. (2019). Delhi Police film protests, runs its image through facial recognition software to screen crowd. The Indian Express. Retrieved from https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/ [15 Feb 2020].

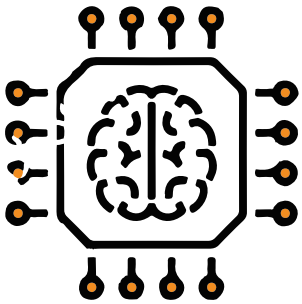
[100] Sengar, M.S. (2019). Facial recognition camera, 5-layer security at Republic Day celebrations n Delhi. NDTV. Retrieved from https://www.ndtv.com/india-news/face-recognition-cameras-5-layer-security-at-republic-day-celebrations-1980969 [15 Feb 2020].

their associates to enabling geo-fencing of suspects. The Uttar Pradesh deployment comes with superior updates that integrates data from all prison, district and state crime records bureaus, and CCTNS. According to the company this instance was the first time that the app carried records of 500,000 criminals that are active in different districts and parts of the state. Trinetra is expected to reach 75 districts, anti-terror squads, and Special Task Force through the android app[101]. Uttar Pradesh was also the first deployment for JARVIS (Joint AI Research for Video Instances and Streams), a "video analytics engine with state-of-the-art facial recognition technology and intelligent monitoring of objects, crowd, perimeters and vehicles". JARVIS was deployed in 70 prisons in the state and includes 3000 security cameras deployed on areas spanning 900 kms[102]. The company claims to have deployed JARVIS with 8 state police departments with vertical expansion into construction, hospitality, banking, and retail[103].

Other profiles of deployment

In 2019 the NCRB released a tender asking for bids to develop the National Automated Facial Recognition System (NAFRS)[104]. This will result in building the world's largest facial recognition system[105]. The aim is to link the NAFRS with the CCTNS in order to integrate the databases for better data analytics and AI deployment[106]. CCTNS by NCRB is a nation-wide networking infrastructure that aims to be a comprehensive database for crimes and criminals, work as a national and state-level database of crime and criminal records, and be a platform for state police to enter details of a crime into the centralised system. One of the stated aims is to achieve the objectives of developing a comprehensive CCTNS are the interlinking of police stations, national and state data centres. The scope of CCTNS has been enhanced to integrate police data with other areas of criminal justice system which include courts, prisons, prosecution, forensics, fingerprint, and juvenile homes to move towards an Interoperable Criminal Justice System[107].

In 2017 the Government of India launched the Digital Police Portal as part of the CCTNS that provides advance search options to police officers and investigators[108]. CCTNS has become an indispensable database for proprietary policing technology to integrate with. Apart



[101] Sangani, P. (2018). STAQU launches AI app for UP police department. ETech. Retrieved from https://tech.economictimes.indiatimes.com/news/mobile/staqu-launches-ai-app-for-up-police-department/67270363.
[102] Mandal, S. (2019). AI for smart crime fighting. Business Today. Retrieved from https://www.businesstoday.in/magazine/the-buzz/ai-for-smart-crime-fighting/story/384515.html [14 Feb 2020].
[103] STAQU. (n.d.). JARVIS. Retrieved from https://www.staqu.com/jarvis
[104] Agarwal, A. (2019). NCRB invites bids to implement Automated Facial Recognition System. Medianama. Retrived from https://www.medianama.com/2019/07/223-ncrb-invites-bids-to-implement-automated-facial-recognition-system/ [15 Feb 2020].
[105] IANS. (2019). World's biggest face recognition system arrives in India next month. LiveMint. Retrieved from https://www.livemint.com/news/india/world-s-biggest-face-recognition-system-arrives-in-india-next-month-11571669785911.html [15Feb 2020].
[106] See Mehrotra, K. (2019). Automated facial recognition: what NCRB proposes, what are the concerns. Indian Express. Retrieved from https://indianexpress.com/article/explained/automated-facial-recognition-what-ncrb-proposes-what-are-the-concerns-5823110/ [15 Feb 2020].
[107] MHA. Crime and criminal tracking network systems. Retrieved from https://www.mha.gov.in/sites/default/files/CCTNS_Briefportal24042018.pdf [15 Feb 2020].
[108] PIB. CCTNS Digital Police Portal launched to fast-track Criminal Justice System in the Country. Retrieved from http://pibarchive.nic.in/mobile/mbErel.aspx?relid=171422 [15 Feb 2020].

Without a legal framework and standards for what qualifies as lawful profiling, a delineation of relevant authority, and attendant powers and procedures there remains an obfuscation of operating procedures which can serve to elide fundamental rights and institutionalise the circumscription of privacy and autonomy without accountability and access to remedy.

from national facial recognition system, many administrative bodies have been implementing facial recognition within their respective jurisdictions. Following the proposal of the Railway Protection Force (RPF) of Bengaluru for the use of facial recognition in Indian Railways, facial recognition system will be fully implemented at the KSR City Railway station. The Union Ministry for Women and Child Development in partnership with the States plans to deploy AI powered CCTV camera in 8 cities (Delhi, Kolkata, Mumbai, Chennai, Bengaluru, Hyderabad, Ahmedabad and Lucknow) in India as a part of the safe city plans[109].

Navigating privacy and security: Considerations on interoperability, data fusion, and operational due diligence

Security and maintenance of law and order have always been limiting arguments for incremental bounding of privacy. Deployment of AI in law enforcement has an overarching influence of facial recognition in crime prevention and investigation. As evinced by the Delhi example, facial recognition is applied on footage of previous protests in the city for future law and order purposes it raises crucial questions about pervasive monitoring of political rallies and its effect on tagging and labelling of data within the policing database which could bias outcomes. The use of facial recognition at a political rally in December came after a wave of protests against the Citizenship Amendment Act, 2019. This raised questions about whether the Delhi Police had used drones as a mechanism to track protestors.

Despite a report by the Press Trust of India over the usage of drone by the Delhi Police, a Right to Information request elicited a denial to the effect from a specific district division of the Delhi Police force which did not unequivocally exclude Delhi Police as an institution that used drones to monitor protests[110]. The deployment of drones in monitoring protests raises questions about authorisation, due process, and necessity and proportionality. Coupled with the use of proprietary technology to conduct multi-modal analysis of biometric data, this throws into sharp relief the lacunae of legal and regulatory safeguards that can establish a framework of lawful profiling and due process to build in transparency and accountability in the system.

The Personal Data Protection Bill, 2019 referred to the joint committee contains carve outs for non-consensual processing (section 12) as well as exemptions which allow the Central Government to exempt any agency of the government from the Act (section 35) as well as for personal data "processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force" (section 36a). This nullifies any protection or recourse offered by the law to the data subject or data

[109] Parashar KM, K. (2018). Smart CCTVs to ensure women safety in Bengaluru. The New Indian Express. Retrieved from https://www.newindianexpress.com/cities/bengaluru/2018/mar/13/smart-cctvs-to-ensure-women-safety-in-bengaluru-1786257.html [15 Feb 2020].
[110] Barik, S. (2020). Delhi Police division denies it used drones to film CAA protestors. Medianama. Retrieved from https://www.medianama.com/2020/02/223-delhi-police-drones-caa/ [15 Feb 2020].

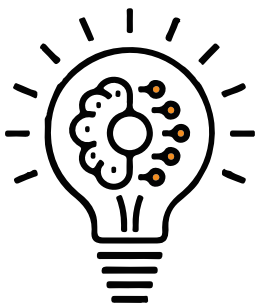
In the integrated application of facial recognition and predictive policing it is unclear whether there is an executive order mandating the deployment or the discretion of individual police departments given the adoption by district level police forces in the country.

principal as referred to the in the Indian context.

However, as per the Srikrishna Committee report which was tasked to draft the data protection bill any intelligence gathering without statutory authorisation and solely on executive order will stand to violate the ruling under the Puttaswamy judgement which declared privacy to be a fundamental right guaranteed under the Indian constitution. However, in the integrated application of facial recognition and predictive policing it is unclear whether there is an executive order mandating the deployment or the discretion of individual police departments given the adoption by district level police forces in the country. However, the non-availability of specific legislative framework like the Police Directives in the European Union raises questions and considerations about the contours of AI and law enforcement landscape.

One of the underlying aims behind deploying predictive and investigative technologies for law enforcement purposes have been the interoperability of isolated datasets in order to have a unified data architecture that helps increase efficiencies in investigation and detection and enables predictive policing. According to estimation by a senior law enforcement official the Aadhaar database will eventually be integrated with AI based policing in order to avoid duplication of efforts to build a parallel system[111]. A move towards interoperability and advanced detection technologies have also driven demand for analysis of multi-modal data beyond biometric data in the form of voice, speech, and gait analysis. This raises questions about the parameters for analysis as well the databases against which real-time data is used to test against.

Moreover, without a legal framework and standards for what qualifies as lawful profiling, a delineation of relevant authority, and attendant powers and procedures there remains an obfuscation of operating procedures which can serve to elide fundamental rights and institutionalise the circumscription of privacy and autonomy without accountability and access to remedy. This is compounded by the fact that there is currently no clarity on level at which an individual's data or record enters the system and how such data is stored. For example, if the police takes a picture of the 'suspect' to run it through a facial recognition system does the system retain that picture and if so, where is it stored[112]. Given that Staqu added other biometric parameters like fingerprints and voice samples to provide surety in the event of failures by facial recognition systems it also raises similar questions about storage of data about non-convicts. Even though the police cannot take photographs of those under trial and accused, according to the Madras High Court the taking of pictures of suspects to match against a criminal database raises questions critical questions about defining legal limits within the increased integration of technology in the criminal justice system.



[111] Sathe, G. (2018). Cops in India are using artificial intelligence that can identify you in a crowd. HuffPost. Retrieved from https://bit.ly/2vd21m0 [25 Feb 2020].
[112] Sengupta, R. (2019). How this Gurugram start-up is helping police, Indian army catch bad guys using AI. YourStory. Retrieved from https://yourstory.com/2019/04/gurugram-startup-indian-army-artificial-intelligence [25 Feb 2020]

Deployment of AI in the education sector is currently at the stage of potential scaling up after a successful pilot. In health, it is at the stage of regulatory development and ecosystem ideation for developing national health data architectures for springboarding AI applications.

Conclusion

Across the cases studies, law enforcement has the maximum scale of application of AI and facial recognition technologies operating within a data rights vacuum. Given, the pervasiveness of automated facial recognition technologies, the absence of regime of legal due process outlining rights and access to remedy underscores the unchecked extent of pervasive discrimination and violation of privacy. While law enforcement and security consideration are often used arguments for qualifying privacy rights, its operation within a legal and regulatory lacunae serves to obfuscate the need to balance of such contending interests. Further, in the absence of an environment for providing rationale for pervasive surveillance and mechanisms for transparency and accountability it undermines trust in public deployment of technology. Given the increased prevalence and rate of integration within operational procedures, it becomes imperative to align operational processes with rights-based principles and protections in order have applied principled procedures.

Recommendations

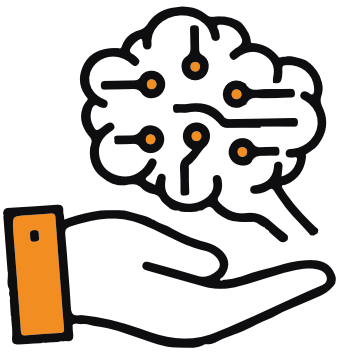
Police guidelines: Draft police guidelines for data processing for law enforcement purposes and use of pervasive technologies like AI for processing data which outlines rights, responsibilities, and conditions; purpose limitation; delineation of the purposes; establishes operational due diligence; defines relevant authority; and incorporates the need for impact assessment and bias detection mechanisms.

Supplier/partner due diligence: Perform an ethics check on the supplier and vendor through algorithmic assessments in order to understand it approach towards predictive algorithms to root out bias.

Open source vs proprietary technologies: Move towards open source vs proprietary technologies in order to ensure secure and inclusive systems by providing transparency and accountability of software operations.

Vetting training data: In order to avoid false positive within the system it is important to vet the training data in order to ensure efficiency and avoid bias in the system.

Identify the stage of entry into the system: Some of the technological deployments documented use facial recognition system on the suspect. It important to determine at what stage an individual enters the system and whether suspects not yet convicted should be a part of the systems given that there is lack of transparency on data sharing, storage, and handling.



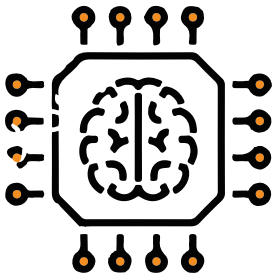
Undertake periodic impact and bias detection assessments:
It is important to test systems to undertake ensure efficiency and accountability. For example, if the system predicts a particular location for predictive policing with a greater frequency than others from where crimes are being registered but has not been signalled within the system and where the causality for such be triangulated within.

FINDINGS

The commonalities and differences identified through the case studies are outlined below:

Differences

- **Stages of deployment:**
  - Deployment of AI in the education sector is currently at the stage of potential scaling up after a successful pilot.
  - In health, it is at the stage of regulatory development and ecosystem ideation for developing national health data architectures for spring-boarding AI applications. Further, given that AI in healthcare has made the most significant advancements in image parsing technology there is proposition of a pilot deployment of a diabetic retinopathy screening mechanism, developed by Microsoft, at Primary Health Centres identified by NITI Aayog.
  - Law enforcement has seen maximum scale of deployment of AI and facial recognition systems in predictive policing and investigations.
- **Types of institutional arrangements:**
  - In education and health, pilot and potential PPP deployment has been through the use of technology provided and systems designed by Microsoft
  - In the case of law enforcement, it is unclear whether the system was designed and procured from STAQU or deployed in collaboration and to what extent it does or does not continue to provide operational support. Further, collaborations with domestic research institutions have also led to deployment in cities like Delhi.
- **Data and datasets used:**
  - In education, data was triangulated from Unified District Information System for Education (U-DISE), containing school infrastructure information and the data on teachers and their work experience, education assessment data from multiple sources, and socioeconomic data from the UIDAI[113] Aadhaar system[114]
  - In health, the aim is to move towards a unified national health architecture that entails the creation of uniquely identifiable patient database based upon a foundation



[113] The Unique Identification Authority of India is the entity mandated to issue the 12-digit Aadhaar number and manage the Aadhaar database.
[114] Srivas, A. (2016). Aadhaar in Andhra: Chandrababu Naidu, Microsoft have a plan for curbing school dropouts. The Wire. Retrieved from https://thewire.in/politics/aadhaar-in-andhra-chandrababu- naidu-microsoft-have-a-plan-for-curbing-school-dropouts [16 Feb 2020].

identification system like the Aadhaar and pooling of health data from public and private sources. The aim is to build NHS on the backbone of the national health resource registry, claims and coverage platform, personal health records, and national health analytics platform with that aim that it works as a presenceless, paperless, and cashless consent layer.

  - In law enforcement, data is matched against Crime and Criminal Tracking Network, digitized police records, facial recognition data from CCTV cameras and potentially drones, biometric data available on file, zonal integrated network system of missing and found children along with the use of multi-modal analytics systems where it is unclear with which databases samples are matched against.

- **Businesses involved:**

  - With regard to AI deployments in education and health Microsoft is most significant player.

  - In law enforcement, domestic company STAQU is the most significant player despite Japan's NEC Technologies having the first mover advantage.

Commonalities

- **Data combination and JAM trinity**: Processes underlying AI deployment across sectors involve the combination of multiple databases with the foundational data stack being built through the triangulation of data through the JAM trinity that includes the ***J****an Dhan* financial inclusion programme, the **A**adhaar biometric database, and **m**obile numbers.

- **Incidence of impact on privacy**: The combination of databases, triangulation of sensitive personal data under the JAM trinity, in tandem with efficiency requirements to uniquely identify each individual raises critical questions about the impact on privacy and security as a result of pervasive surveillance through multiple nodes without purpose limitation as well an increased risk interface respectively.

- **Individual vs community data**: The Srikrishna Committee Report which formed the background of the draft personal data protection bill, 2018 identified a category of data called 'community data' which "challenges the notion of individual control over her own personal data". The e-commerce policy of 2019 contained a proposal to promulgate rules that would enable to boost the competitiveness of the e-commerce sector. Reading this in light of the data sovereignty discourse of India's data for India's development and in conjunction with

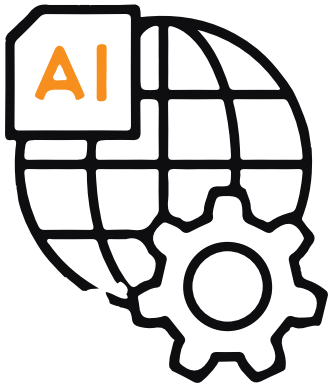
section 91(2) of the 2019 iteration of the draft data protection bill containing the provision that

> The Central Government may, in consultation with the [Data Protection] Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed

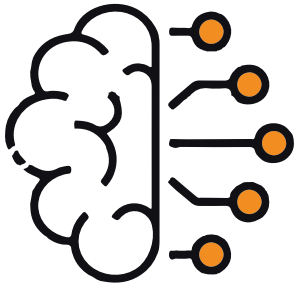
Undergirds the moves towards aggregating data sets, creating data sets with unique identifiers, minimising individual control and autonomy over their data, and rationalising moves towards weakening data protection regimes in favour of a wide ambit for non-consensual government processing.

- **Hybrid institutional arrangements**: AI deployment have been through hybrid institutional arrangements with the private sector and academia without clear delineations about data sharing, handling, storage, and future analytics and ownership of such knowledge products.

- **Conflicts and gaps within data governance regimes**: Deployments contain attendant gaps between different data governance regimes. Despite the recognition of privacy as a fundamental right, legal provisions for data privacy and protection are still at a nascent stage or lacking. Without the absence of a data protection law in place, sections 43 and 43(a) of the Information Technology Act, 2000 provide limited privacy protections in the way of seeking damages for unauthorised access of data. The draft data protection bill, with its carve-outs and exceptions, do not provide hope for respite. The e-commerce policies (2018; 2019) underscore the notion of community data to service India's digital economy by servicing the data requirements faced by technology start-ups in the country. The Digital Information Security in Healthcare Act (DISHA), 2018 does not address the question of government storage of DNA data under the DNA Technology (Use and Application) Regulation Bill, 2018 for criminal justice purposes. According to section 27 of the draft data protection bill, a data fiduciary cannot process biometric data without undertaking an impact assessment, further according to section 92 "no data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law". Further, it is not clear whether such institutional arrangements can potentially fall under the purview of being a 'significant data fiduciary' under section 26(1) of draft data protection bill, 2019 where the Data Protection Authority will be able classify the a data fiduciary as significant data fiduciary based on: (a) volume of the data processed; (b) sensitivity of personal data processed;



(c) turnover of data fiduciary; (d) risk of harm by processing by data fiduciary; (e) use of new technologies for processing; (f) any other factor causing harm from such processing. Or whether such processing would be exempt through discretionary powers of the Central Government or fall within the ambit of non-consensual processing as being the vehicle for 'government functions'.

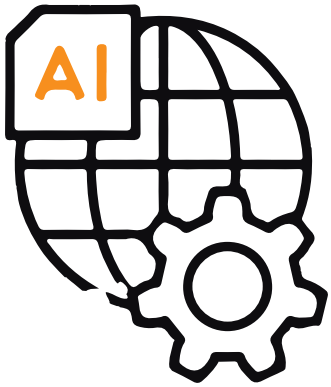


- **Lack of foundational safeguards**: Conflict and gaps within differing data governance regimes weaken the foundational safeguards afforded to an individual vis-à-vis the state and businesses and provide inadequate rights towards protection and remedy in the case of risk of and actual harms. Given, the impact of erosion of rights under emerging systems are invisible and pervasive under emerging technologies like AI a strengthening and harmonisation of a data rights regime is urgently required.

CONCLUSION

The rapid integration of AI in social, economic, and administrative systems in India require critical understanding of the objectives, dynamics, and modalities of the cases of deployment and their commonalities and divergences. This helps to move towards developing contextually sensitive working principles, guidelines, and frameworks inductively derived and abstracted from empirical evidence. This would help towards the operationalisation of rights-based frameworks for responsible automated systems with greater transparency and accountability. The different stages of deployment delineated above underscore an overarching commonality of large scale data combination across sectors with a move towards building national data architecture that provides a 360 degree view of all individual parameters of economic and social interaction - i.e. the IndiaStack. Driving active AI deployment initiatives are moves towards pervasive datafication that serve as the impetus towards realisation of such a data repository and architecture. Like the use of facial recognition in Tamil Nadu to mark student attendance[115], surveillance tagging of sanitation workers in Haryana[116], proposed use of facial recognition in Telangana for voter verification in local elections[117], and voluntary airport check-in using facial recognition at the Kempegowda International Airport in Bengaluru, Karnataka among others[118].

Giving the discursive legtimisation for such realisation are the conceptualisations of data sovereignty and community data that undergird data and digital policy-making in India. The concept of data sovereignty entails the use of India's data for India's people. At the G20 meeting in Japan, Union Minister for Railways and Commerce said that data is a sovereign asset and that personal, community, and public data generated in the country should be be used to service the welfare and development of its people[119]. This conceptualisation has translated to data localisation mandates so that Indian start-ups can have easier access to data as put forward in the national e-commerce policy, 2019[120] and its earlier more controversial iteration of 2018[121] which contained the proposition that localised data in India will be available for start-ups

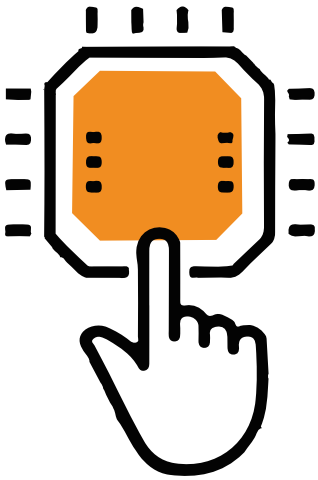


[115] Pon Vasanth B.A. (2019). Facial recognition attendance system in two Chennai schools. The Hindu. Retrieved from https://www.thehindu.com/news/cities/chennai/face-recognition-attendance-system-in-two-city-schools/article29412485.ece [23 Feb 2020].
[116] Khaira, R. (2020). Surveillance slavery: Swachh Bharat tags sanitation workers to live-track their every move. HuffPost. Retrieved from https://www.huffingtonpost.in/entry/swacch-bharat-tags-sanitation-workers-to-live-track-their-every-move_in_5e4c98a9c5b6b0f6bff11f9b [23 Feb 2020].
[117] Al Jazeera. (2020). India's Telangana to test facial recognition in local elections. Retrieved from https://www.aljazeera.com/news/2020/01/india-telangana-test-facial-recognition-local-elections-200122093408249.html [23 Feb 2020].
[118] Tech Desk. (2020). DigiYatra to bring facial recognition system to airports: Here's how it works. Indian Express. Retrieved from https://indianexpress.com/article/technology/tech-news-technology/digi-yatra-is-bringing-facial-recognition-system-to-airports-heres-how-it-will-work-6230101/ [23 Feb 2020].
[119] Ranganathan, N. (2019). The seduction of data sovereignty in India. Hindustan Times. Retrieved from https://www.hindustantimes.com/analysis/the-seduction-of-data-sovereignty-in-india/story-iOS8cVKxstIIgJLy47Iy0J.html [24 Feb 2020].
[120] DPIIT. (2019). Draft national e-commerce policy: India's data for India's development. Retrieved from https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf [24 Feb 2020]
[121] DPIIT. (2018). Electronic commerce in India: Draft national policy framework (leaked). Retrieved from https://www.medianama.com/wp-content/uploads/Draft-National-E-commerce-Policy.pdf [24 Feb 2020].

Giving the discursive legtimisation for such realisation are the conceptualisations of data sovereignty and community data that undergird data and digital policy-making in India. The concept of data sovereignty entails the use of India's data for India's people.

which meet the stipulated criteria of turnover of Rs. 50 crore (approx. $6 million). Post the backlash against 2018 policy, Ramesh Abhishek, Secretary, Department for Promotion of Industry and Internal Trade (DPIIT) said that there was actually no need for a policy when one can do the things that have been identified. However, a more elaborate and watered down version of the E-Commerce Policy was released in 2019 but leaves the question open in terms of government action and accountability towards and within such initiatives. Therefore, in order to understand current and future directions of policy for emerging technology and ascertain and provide for rights-based implications, it becomes important to take into account the priorities and objectives of data governance across different sectors. This will help to understand and map out the incidence of impact and comprehend to what extent the foundation on which pervasive technologies like AI are to be predicated are robust enough to withstand the challenges that such systems will throw up.

In order to arrive at frameworks and instruments for responsible automated systems, it becomes important to first map out domestic cross-sectoral policies that can have a potential impact on data governance in conjunction with national data protection frameworks. Understanding the current domestic framework will enable to assess the gaps in achieving international standards for responsible automated systems and balancing for the needs and interests of different stakeholders. This gap identification will then enable to chart out the future course of action by providing an indication of the nature and kind of advocacy required to arrive at process and outcomes that centre rights and accountability along with innovation and efficiency. Recognising the urgent need for empirical and evidence-based social research in this area, this report aims to form the foundation for DEF's sectoral deep dives and empirical social research in this area in contributing towards gap analysis, rights-based implications of automated decision-making systems, and working to mainstream a business and human rights framework within policy - making around emerging technologies.



RECOMMENDATIONS

For government

- Harmonisation of policies on data governance across different sectors
- Transparency reports on aggregation of databases
- Develop a process document on selection of business for PPPs along with standards of service and considerations and safeguards of
- Put service agreements under PPPs in the public domain with a note on
    - How data fiduciary relationship and responsibility is determined within the such institutional arrangements
    - Clear definition of functions of such deployment
    - Clear statement whether or not it comes under the purview of 'government functions'
    - Clear statement on whether such an entity has exemption under the Act from the Central Government and the rationale
- Adopt a government-wide principles document for policy-making for data governance and AI
- Establish supplier standards and protocols for compliance under PPP institutional deployments
- Clarify definitions and delineations of individual vs community data

For businesses

- Ensure transparency in PPP service agreements to ensure accountability in automated systems; data sharing, storage, and usage; and steps to safeguard rights within systems design
- Develop operational policies, procedures, and safeguards for automated systems that follow principled processes
- Use representative datasets and bias detection mechanisms for automated systems that include social and technological audit
- Commitment to establish and sustain internal due diligence and compliance procedure for automated systems and produce annual compliance/ accountability reports of its automated systems deployments
- Compliance reports should contains disclosures about PPP partnerships, terms of reference, and sectors of deployment

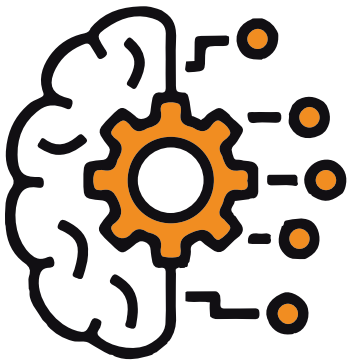
- Investors should encourage businesses that are able to demonstrate human rights compliance within their deployment of automated systems

For civil society organisations

- Develop accountability standards and framework and advocate for a standardised model of reporting and compliance, providing for sectoral contextualisation
- Developing empirical evidence based studies for understanding the impact of deployment of AI technologies on citizen, especially marginalised and underserved citizen groups
- Develop rights-based guiding principles for policy-making
- Advocate for narrower definitions and remit of non-consensual processing
- Work on intra-stakeholder group solidarity and bridge building with civil society organisations working on a diverse range of issues to align privacy concerns within data governance

For multi-stakeholder initiatives

- Advocate for multi-lateral business and human rights instrument for automated decision-making systems
- Advocate for adoption of standardised reporting and compliance mechanisms
- Work towards driving consensus on accountability standards and frameworks
- Work towards bringing together civil society organisations and business to co-develop mechanisms for social and technological audit
- Driving regional/ national working groups to understand global counters of the issue and facilitate learning, knowledge-sharing, and network building



Digital Empowerment Foundation

House no. 44, 2nd and 3rd Floor, Kalu Sarai
New Delhi – 110016

Tel: 91-11-42233100 / Fax: 91-11-26532787

Email: def@defindia.net | URL: www.defindia.org