Towards AI sovereignty: The good, the bad, and the ugly of AI policy in India

Jai Vipra
Non-Resident Fellow, CyberBRICS project, Center for Technology and Society (CTS), Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro; and PhD Student, Department of Science and Technology Studies, Cornell University, Ithaca, New York
https://orcid.org/0009-0007-6220-0154

Abstract

India's approach to artificial intelligence (AI) policy reflects a mix of ambition, creativity, and inconsistency. While the country has made significant strides in areas such as computational capacity, data protection fundamentals, and connectivity, its AI sovereignty efforts are hampered by a lack of strategic coherence, inadequate cybersecurity, and an absence of algorithmic-accountability legislation. This article evaluates India's AI policy through the lens of the key AI sovereignty enablers (KASE) framework (Belli, 2023; CyberBRICS, 2024), highlighting positive precursors, opportunities for improvement, and fundamental shortcomings of the Indian approach. It argues that India's reactive and fragmented policymaking, coupled with frequent shifts in direction, undermines its potential to achieve AI sovereignty. The article concludes with recommendations for a more cohesive and forward-looking AI strategy that aligns with India's long-term interests.

Keywords

artificial intelligence (AI), AI sovereignty, India, policy, computational capacity, data protection, connectivity, cybersecurity, algorithmic accountability

DOI: https://doi.org/10.23962/ajic.i35.21263

Recommended citation

Vipra, J. (2025). Towards AI sovereignty: The good, the bad, and the ugly of AI policy in India. *The African Journal of Information and Communication (AJIC)*, 35, 1–11. https://doi.org/10.23962/ajic.i35.21263

1. Introduction

In April 2023, the Indian Ministry of Electronics and Information Technology (MeitY) stated in response to a parliamentary question that it was not planning to regulate artificial intelligence (AI), and that it sought to promote the growth of the sector in India (Singh, 2023a). In July 2023, the Telecom Regulatory Authority of India (TRAI) recommended urgently setting up a regulatory framework for AI (Aulakh, 2023). The next year, in March 2024, MeitY issued an advisory that included a provision requiring technology firms that were deemed "significant" to obtain government permission before releasing AI models (MeitY, 2024). The advisory was not meant to be legally binding. Fifteen days later, responding to criticism, the government withdrew this part of the advisory and thus no longer required firms to obtain permission before releasing AI models (Agrawal, 2024).

These instances are emblematic. India's approach to AI regulation and AI sovereignty has been characterised by infectious enthusiasm, creditable ambition, and even some good policies, but a lack of strategic coherence or overarching vision. Much AI-related policymaking in India has been in reaction to matters in which the government has had a political interest, such as in the representation of certain politicians by large language models (LLMs), resulting in frequent changes in direction.

This article aims to provide a broad overview of India's policies on, and with relevance to, AI, and to assess how these policies relate to AI sovereignty. I adopt a definition of AI sovereignty based on the key AI sovereignty enablers (KASE) framework set out in Belli (2023), in terms of which AI sovereignty is the ability of a country to "understand, develop, and regulate AI systems" in order to exercise "control, agency, and self-determination" over them. The KASE framework treats AI sovereignty as a stack, with the overall effect of reducing the unilateral impact of foreign actors on the country's choices (Belli, 2023; CyberBRICS, 2024). To identify and evaluate India's AI sovereignty stack, I map India's policy—both in its status quo and in its recent developments—along the KASE elements, which are:

1. Sound personal data governance;
2. Sound algorithmic governance;
3. Strong computational capacity;
4. Meaningful connectivity;
5. Reliable electrical power;
6. A digitally literate population;
7. Solid cybersecurity;
8. An appropriate regulatory framework, and
9. AI-ready digital public infrastructure.

The first eight KASE elements listed are from Belli (2023), and the ninth—AI-ready digital public infrastructure—was added by CyberBRICS (2024).

I evaluate India's AI policy measures in terms of whether they are positive precursors, opportunities for improvement, or fundamental shortcomings towards the goal of AI sovereignty, based on the KASE elements listed above. There is no clean separation between the categories of precursors, opportunities, and issues; they are instead on a continuum of beneficial or not for AI sovereignty. India's performance on KASE elements is evaluated both in terms of the historical evolution of these elements, as well as the paths that they open up for AI sovereignty in the future. I demonstrate India's mixed, sometimes inconsistent, and evolving approach to AI sovereignty, which can be linked to the government's domestic-capital-directed approach to sovereignty in general (Varadarajan, 2025). I then conclude that this mixed approach has led to a situation where India's dependency on foreign technological developments is only sometimes negated by domestic developments, and that the latter often fall short due to a lack of overarching strategy.

2. An overview of AI policy in India

Policy analysts have referred to India's approach to AI policy as being both oscillatory and broadly pro-innovation (Mohanty & Sahu, 2024). Mohanty and Sahu (2024) also show how a multiplicity of ministries and agencies regulates AI applications and articulates AI policy stances in India.

A few key policy initiatives and documents frame AI policy discussions in India. One of these is a 2018 report by NITI Aayog (a government think-tank), called National Strategy for Artificial Intelligence (NITI Aayog, 2018). This report identifies resource and policy constraints to equitable access to AI, and recommends investments in research, skilling, security, privacy, and promoting AI adoption, as well as closer collaboration with the private sector. In 2021, NITI Aayog followed up with a two-part report on responsible AI, outlining principles for responsible AI in India and setting out methods to operationalise these principles (NITI Aayog, 2021a; 2021b). The first part of the report assesses the direct and indirect impacts of AI, which lead to systems and societal considerations. The second part recommends actions to be taken by the government (providing an appropriate regulatory environment, etc.) and the private sector (incentivising ethics, etc.).

The flagship policy and spending vehicle of the Indian government for AI is the IndiaAI mission. Launched in March 2024, this mission aims to catalyse AI innovation by encouraging investment in, and to some extent subsidising, the various inputs to AI: computational power, data, skills, finance, and ethics frameworks (IndiaAI, n.d.; Prime Minister of India, 2024). In 2025, MeitY published a report on AI governance guidelines development (MeitY, 2025a). The report urges that AI actors be seen as constituting an ecosystem, and recommends the effective enforcement of existing laws, traceability and transparency for regulators, and a central policy coordination mechanism for AI. This last recommendation in particular might address the oscillatory nature of India's AI policymaking.

3. Promising precursors

India has made uneven progress along the KASE framework. The progress on some of these enablers has been remarkable and worth highlighting. Indian AI policy, and its digital policy more broadly, has often been characterised by creativity and unorthodoxy. This section highlights the elements of the KASE framework in which Indian AI policy has particularly excelled in its attempts to make policies with fresh perspectives. These elements serve as examples of the potential of Indian AI policy to serve sovereignty objectives—a potential that, as we shall see, remains largely unrealised.

Proactive policy on computational power

Adequate computational capacity is crucial for training and running AI models, and for conducting AI experiments. India has a comprehensive and flexible computational-power policy set that has gone through productive iterations. Computational policy is a domain in which changes in orientation have been appropriately responsive to changing conditions, rather than being reversals of hastily made policy. India's efforts to build effective computational capacity for AI have three main prongs, which I now discuss in three sub-sections.

GPU procurement subsidy

Many of today's AI models need to be trained on, and also often run on, graphics processing units (GPUs). As part of the IndiaAI mission, the government has allocated around INR50 billion (approx. USD584 million) to partially subsidise the procurement of GPUs for Indian companies (Mishra, 2024). This planned subsidy is meant to be demand-driven, in that the companies will decide the kinds of GPUs that they need to procure, and the government will ensure that the purchases that it subsidises are not misused or resold. There is debate in India around the exact model of government spending that can reliably catalyse AI innovation (Suraksha & Lohchab, 2024). Such a debate has led to a change in stated government policy from the creation of a GPU cluster through government procurement to the current policy of subsidisation (Prime Minister of India, 2024). At the time of writing, in early 2025, the government is about to launch a portal to help businesses, non-profits, government organisations, and others to access subsidised use of 18,000 GPUs (*BW Businessworld*, 2025).

Production- and design-linked incentive schemes (PLIS and DLIS)

In the period 2021–22, the government unveiled production- and design-linked incentive schemes (PLIS and DLIS, respectively) to subsidise the production and design of semiconductor chips in India (MeITY, 2023b). Since India does not possess the technology or know-how to design or produce advanced GPUs, these schemes target the design and production of chips that lag behind the frontier but are nevertheless useful. Under these schemes, the government reimburses up to 50% of costs (and incentivises a portion of sales) for companies that are majority Indian-owned in order to nurture a domestic ecosystem for compute power (MeitY, n.d.). These programmes have not had the expected level of success, particularly due to the reluctance of foreign semiconductor producers and designers to transfer technology, and due to the nascent level of the semiconductor market in India (Vipra, 2024). Nevertheless, these schemes demonstrate that Indian policymakers understand the importance of domestic capabilities in chip design and production.

Modernising the state-owned Semi-Conductor Laboratory (SCL)

In 2023, the government invited proposals to modernise the state-owned SCL (MeitY, 2025b). The state expects such modernisation to follow one of, or a combination of, two broad paths: turning SCL into a research and development hub, and/or turning it into an at-scale manufacturer of chips. At present, SCL produces older semiconductor models at a relatively low volume, but these chips are critical for India's defence needs. In an environment where chip design and production are concentrated in a few private companies outside India, this focus on developing the capabilities of a state laboratory is an important pillar of India's efforts towards AI sovereignty.

Useful data-governance experiments

While numerous countries now have data-protection laws that look broadly similar, the laws' philosophical and practical foundations differ. In India, the Digital Personal Data Protection Act of 2023 recognises data protection as a fiduciary duty (Republic of India, 2023). This means that the entity that collects or uses personal data must observe a duty of care towards the "data principal", i.e., the person to which the data pertains, and must act in the person's best interest. This requirement to act in the data principal's best interest has the scope to be interpreted in ways favourable to people, rather than corporations, even if the technology, manner, or purpose of data use changes. Specifically, in the case of AI, such a foundation opens up avenues to challenge the use of personal data to train AI models that eliminate jobs, undermine individual intellectual property, and/or degrade public or private services. In this respect, a *fiduciary* relationship is a better approach than an approach based on data as *property*, of which people can be dispossessed through unequal power relationships.

However, as is explained later in this article, other aspects of India's data protection law undermine Indians' right to privacy in the context of widespread AI use. In addition, as Bailey and Goyal (2020) point out, the use of the term "data fiduciary" has not translated into fiduciary-like obligations in the law for technology companies. Prasad (2019) presents some options to invoke fiduciary obligations, for instance, on large technology companies, but also concludes that provisions in the data protection law do not correspond to fiduciary-like obligations.

India has also experimented with other data governance practices that have the potential to protect AI sovereignty. For instance, Indian regulators like the Reserve Bank of India have had strong stances on data localisation, requiring that some types of data be stored locally in India (Reserve Bank of India, 2018). Local data storage requirements in select cases might ensure that data protection rules are more effectively applied to the data. Such requirements might also create more opportunities to build AI sovereignty by providing leverage for international negotiations on digital issues, much like national control over other resources such as minerals. Multinational technology firms prefer no local storage requirements, and countries like India use data localisation as a non-ideal method of regaining national rights over data (Basu, 2025).

Another example is India's consent management framework. Section 2(g) of India's Digital Personal Data Protection Act, 2023, provides for an intermediary called a consent manager, which enables a person to "give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform" (Republic of India, 2023). The Act holds consent managers accountable to data principals (section 6(8)). Consent managers are expected to help data principals to avoid consent fatigue and provide interoperability (Kazia et al., 2025). Like consent managers, account aggregators in the financial sector aim to provide seamless flows of financial services data (Kazia et al., 2025). Whether data is actually a resource or not, the consent management framework recognises that data is used like a resource and attempts to shape a more equitable market for this resource-style use by allowing data to be transferred according to the wishes of the data principal. This is in contrast to the dominant model where, once data is collected, people have little to no control over its movement.

Respectable connectivity foundations

According to government statistics, India has 954 million internet subscribers, which is about 68% of India's population (Ministry of Communications, 2024). The average data cost fell by almost 100% in the period 2014–24, and 4G coverage of remote villages in difficult terrains neared 25% in the same period (Ministry of Communications, 2024). Through a mobile-first strategy, India has managed to connect millions of people to the internet in a short period of time.

Indian policymakers and regulators also seem to be prepared for new issues arising from the connectivity infrastructure requirements of digital technology. The Telecom Regulatory Authority of India (TRAI) has recently studied India's domestic ownership and capabilities in submarine cables and landing stations, noting that regulatory complexity has made it difficult to conduct business in this sector (Arya, 2021; TRAI, 2023). India has also opened up the space sector to private players, encouraging innovation in satellite and other related communications infrastructure (ISRO, 2023).

Caveats regarding good policy

One aspect to note in relation to all the policies I have classified here as "promising precursors" is that they are not necessarily tied to other policy measures such that they might work together towards the goal of AI sovereignty. The provision of computational capacity would return more dividends if it were paired with appropriate investments in AI education, such that the computational capacity is used optimally and to its potential. Such use is not guaranteed through the mere provision of resources. In a world where computational power is expensive and relatively scarce, investments in using it optimally require multi-pronged approaches. Similarly, data policy must go beyond the "unlocking", "leveraging", or "making available" data for AI that is so often foregrounded in policy documents and business documents aimed at policy changes (Gupta, 2025; Saxena, 2021; Singh et al., 2025; Suri, 2025).

Strong data protection laws—which, for instance, ban surveillance pricing where companies price goods individually based on data collected—can make such practices prohibitive. The discouragement of this tendency of targeted advertising and pricing, engaged in by platform business models, could perhaps redirect AI innovation towards more productive and public-interest endeavours. At the very least, it can spur experimentation with newer business models. Opening up the space sector to private players and presenting India as a space-investment destination (Modi, 2025) is not necessarily wrong, but must be accompanied by careful national security and sovereignty considerations. Not protecting against ceding control of communications infrastructure to foreign players is ill-advised in a digital economy.

4. Opportunities for improvement

Connectivity gaps

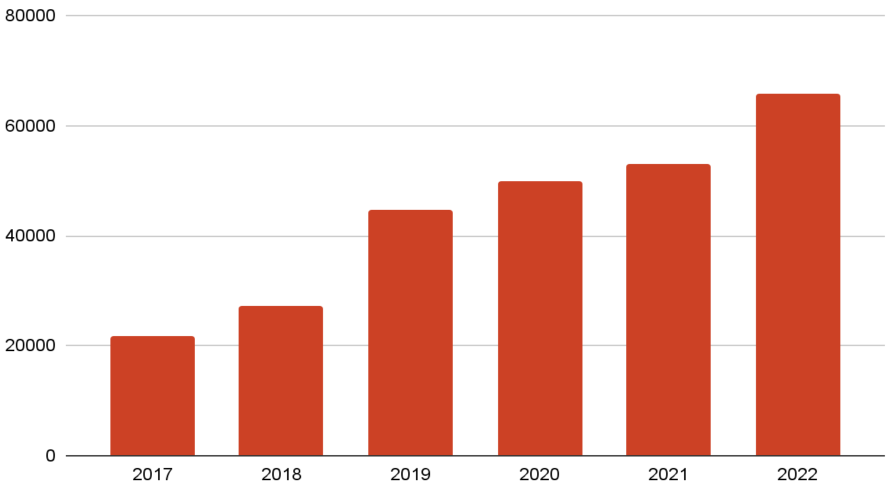
Much of India's increase in connectivity over the last decade has been the result of a price war among providers that is leading to the monopolisation and subsequent ill-health of the telecommunications market in India (Chandrasekhar & Ghosh, 2021). In other words, connectivity has been provided to a large proportion of the population by increasing monopolisation in the telecommunications sector, which might also threaten market competition in other sectors through the control of data in the telecommunications sector (Chandrasekhar & Ghosh, 2021). Thus, while connectivity gains have been achieved through this price war, the manner of their achievement might yet impose costs on consumers in the future.

According to a government survey conducted between 2018 and 2020, only a third of Indian women had ever used the internet, compared to more than half of Indian men (McDougal et al., 2022). Rural women are held back from the internet even more, with only 3 in 10 women having ever accessed the internet (Sheriff, 2020). Regional disparities in access are significant. In the national capital, there are 186 internet subscribers per 100 people (many individuals have more than one subscription), while in the state of Jharkhand, there are only 10 internet subscribers per 100 people (Parsheera, 2022). In all states, except Kerala, urban areas have a higher internet subscription density than rural areas (Parsheera, 2022). As long as access to the internet and therefore to AI technology is unequal, the government cannot achieve unbiased, fair outcomes of AI use.

Inadequate cybersecurity

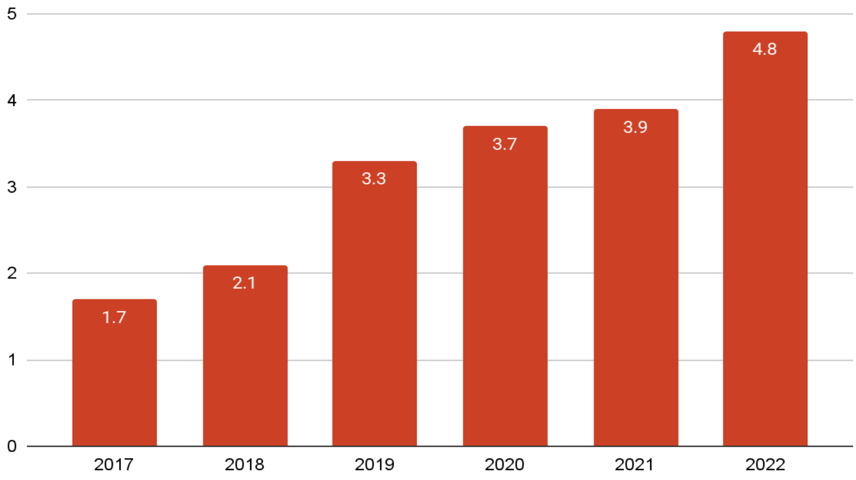
An important dimension of AI sovereignty is a country's ability to ensure the security of its AI systems and of critical infrastructure where AI is embedded. A country must be able to govern crime that occurs through digital means; with the proliferation of AI, such crimes become easier to commit and scale, through methods such as voice-cloning (Hernandez, 2023). India faces a large number of cyberattacks, and its cybersecurity strategy does not seem to be keeping pace. It ranks 47th in terms of preparedness in a composite cybersecurity index (SEON, 2023). According to one index, India was the 10th largest hotspot of cybercrime in the world (Bruce et al., 2024). Figures 1 and 2 below show that cybercrime has been steadily rising in India in recent years.

Figure 1: Cybercrimes in India (annual totals)



Source: Compiled by author based on data from National Crime Records Bureau (NCRB) (2018–2023)

Figure 2: Cybercrimes in India (annual totals per 100,000 people)



Source: Compiled by author based on data from NCRB (2018–2023)

India's legal framework for cybersecurity includes some provisions in the Information Technology Act, 2000, the Digital Personal Data Protection Act, and guidelines by sectoral regulators (MeitY, 2025a). These provisions and their current enforcement mechanisms may be inadequate to deal with the scale and sophistication of the cybersecurity threats that generative AI might lead to (MeitY, 2025a). Despite the statistics cited above, the IndiaAI mission does not include a strong focus on cybersecurity. Moreover, the draft National Cybersecurity Strategy, prepared in 2021 and reformulated in 2023, has not yet been adopted (ETTelecom, 2023). Also, there are no specific protection policies for India's AI-related infrastructure, and there is an ongoing administrative conflict between different departments over the governance of India's nodal cybersecurity agency, the Indian Computer Emergency Response Team (CERT-In) (Barik, 2024).

Narrow AI talent and education policies

Many of the individual policies that comprise India's AI strategy focus on talent development and education. For instance, the IndiaAI mission has a component called FutureSkills, which plans to increase AI programmes at all levels of education and includes a focus on AI courses in smaller cities (IndiaAI, n.d.; Prime Minister of India, 2024). The MeitY IndiaAI Expert Group has recommended the creation of a model curriculum for AI, "upskilling" the non-IT workforce, faculty training in AI, encouraging faculty to collaborate with industry, and the creation of an India-specific AI community (MeitY, 2023). There are various government funding mechanisms for AI training and Centres of Excellence in educational institutions. The Department of Science and Technology has instituted technology innovation hubs in various colleges (DST, n.d.).

Despite AI talent and education policies that appear to tick all the necessary boxes, India's approach lacks strategic direction. Many engineers and scientists who work at the foremost AI companies in the world have studied at Indian institutes, but a large proportion of Indian AI scientists prefer to work in the United States (Zwetsloot et al., 2021). Nonetheless, globally India ranks second in terms of AI talent, behind only the US (Mostrous et al., 2024). That this high prevalence of AI-relevant skills is not translating into global leadership in AI innovation for India is a policy failure. A reading of policy documents, including the IndiaAI expert group recommendations referred to above, shows that India's AI talent and education policies are limited to training students and workers in the technology and methods already developed in other countries, rather than promoting the development of new AI technology and methods in India. India can do much more with its large science and technology talent base, including the public funding of ambitious projects like AI development beyond deep-learning methods towards more fundamental explorations into other approaches to AI.

5. Fundamental issues

Absence of algorithmic accountability

Algorithmic accountability is a critical KASE pillar. Algorithms and their functioning can both lead to social problems, and be instruments of regulation (Belli, 2023). Despite the proliferation of algorithmic decision-making in various parts of daily life in India, and the emergence of AI technology that is likely to increase this prevalence, India does not have any laws that provide for the general governance of algorithmic decision-making. Some sectoral regulations govern a narrow slice of activity, for instance, the regulation of software as medical devices (Lenin, 2024). A proposed Digital India Act is likely to contain provisions on algorithmic transparency and periodic risk assessments, but its introduction has been repeatedly delayed (Sur, 2024). The vast majority of algorithmic decision-making remains ungoverned. It is particularly concerning that AI-driven state surveillance is conducted without a clear legal basis, such as through the use of facial recognition technology by the police, or through the use of a Covid-19 contact-tracing app made mandatory in many contexts during the pandemic (Bhandari & Rahman, 2020; Jauhar, 2021).

In the past few years, Indian gig workers have protested against the arbitrary blocking of their accounts, opaque rating systems, unilateral changes in payment structures, and burdensome requirements to prove eligibility for monetary incentives (Singh, 2023b). Gig workers in India work much longer than eight-hour days, are locked into platforms due to penalties for rejecting gigs, and make far less than minimum wage. The commonality driving these elements of exploitation is management through algorithms that are increasingly AI-driven. Algorithmic management is not limited to platform work—call centre workers, IT employees, and even lawyers are also subjected to granular, digitalised control over their work. Similarly, algorithms affect medical decisions, financial markets, and criminal justice in India, and underpin its surveillance architecture, in particular the use of facial recognition technology at airports and by law enforcement.

Weak data protection

While the robust approach to data protection in India, grounded in fiduciary responsibility, has been outlined above, the actual data protection law fails to rise to the challenges of widespread AI use. The Digital Personal Data Protection Act does not apply to personal data that is made publicly available (Article 3(c)(ii)). This means that no protections are available for such data, including protection against the use of this data for training AI models in ways that potentially violate the principles of purpose limitation and data minimisation (Pahwa, 2023). People who post data, creative work, or intellectual work on the internet do not do so with the expectation that this work will feed into the training of AI models, particularly without compensation. India's data protection law also does not enshrine any rights in relation to automated decision-making, unlike many other data protection laws around the world (Apacible-Bernardo et al., 2023). With AI being implemented to automate decisions across various sectors, this omission is significant.

Frequent internet shutdowns

Another aspect of Indian technology policy that casts a shadow on its ambition for growth and inclusion is the frequent state-directed internet shutdowns. India consistently has the highest number of internet shutdowns globally. Table 1 below, based on data from Access Now (n.d.), shows the annual number of internet shutdowns in India between 2016 and 2023, compared to the country with the second-largest number of shutdowns in the same year. Since Access Now started collecting annual data on internet shutdowns in 2016, India has always had the highest number.

Table 1: Internet shutdowns in India and in country with the second largest no. of shutdowns

Year	No. of shutdowns in India	Shutdowns in the country with second-largest no.	Country with second-largest no. of shutdowns
2016	30	8	Pakistan
2017	69	10	Pakistan
2018	134	13	Pakistan
2019	121	12	Venezuela
2020	108	6	Yemen
2021	106	15	Myanmar
2022	84	22	Ukraine
2023	116	37	Myanmar

Source: Compiled by the author using data from Access Now (n.d.)

India's shutdowns tend to be concentrated in specific regions. For instance, more than 60% of the country's internet shutdowns in 2022 were imposed in Jammu and Kashmir, a region subject to militarisation and crackdowns on political activity (Mogul, 2023). It is difficult to argue that digital services, including AI services, can be provided in a reliable, non-exclusionary, and unbiased manner in a country that is subjected to so many internet shutdowns.

6. Conclusions

It has become clear that some policy areas require more urgent attention than others, while all policy areas could benefit from greater inter-linking and orientation towards common goals. India could benefit from a more explicit political understanding of global AI dominance and AI political–economic sovereignty, and how to leverage its relationships with the US, China, and the EU to protect its own interests. Public subsidies for computational power are potentially good, but we should be careful not to shift the risks of AI-building to the public sector, while allowing the private sector to capture the rewards through building applications that may not be in the public interest. Options for government equity and benefit-sharing are currently underexplored in India's provision of public financial support to private-sector AI development.

Finally, it is inadvisable for India to merely follow the lead of the US (and, indeed, other countries including China and the EU nations) in both technology and technology policy. US technology policy is (understandably) in flux, with priorities shifting from one administration to the next. For instance, antitrust, which was a priority for the Biden administration, is not a priority for the current Trump administration. Meanwhile, India continues work on its Digital Competition Bill (Kumar, 2024). Realities of concentration in AI and digital markets have not changed, and with a revival of mergers, acquisitions, and overall monopolisation in the US, Indian policymakers need to redouble their efforts towards promoting competition domestically.

Acknowledgements

The author thanks Luca Belli, Larissa Galdino de Magalhaes Santos, Amrita Sengupta, Mila Samdub, and two anonymous reviewers for their comments and suggestions.

Funding

Funding for this study was received from the FGV Law School's 2024 CyberBRICS Fellowship Program.

Data availability

The data supporting the results of this study is available upon written request to the author at jv474@cornell.edu

AI declaration

The author did not use any AI tools for conducting the research or writing the article.

Competing interests declaration

The author has no competing interests to declare.

References

Access Now. (n.d.). *Ending internet shutdowns.* Retrieved February 11, 2025, from https://www.accessnow.org/issue/internet-shutdowns

Agrawal, A. (2024, March 15). In revised AI advisory, IT ministry removes requirement for govt permission. *Hindustan Times*. https://www.hindustantimes.com/india-news/in-revised-ai-advisory-it-ministry-removes-requirement-for-government-permission-101710520296018.html

Apacible-Bernardo, A., Sonkar, S., & Chakraborty, S. (2023). Top 10 operational impacts of India's DPDPA – Comparative analysis with the EU General Data Protection Regulation and other major data privacy laws. International Association of Privacy Professionals. https://iapp.org/resources/article/operational-impacts-of-indias-dpdpa-part6

Arya, A. (2021). Submarine telecommunication cable infrastructure regime in India: An analysis on the Indian legal and regulatory regime. *The Indian Journal of Projects, Infrastructure, and Energy Law*, *1*(1), 102–114. https://ijpiel.com/wp-content/uploads/2022/02/9_Submarine-Telecommunication-Cable-Infrastructure-Regime-in-India.pdf

Aulakh, G. (2023, July 20). *Trai recommends regulatory framework for AI, risk-based framework for AI specific use cases*. Mint. https://www.livemint.com/technology/tech-news/trai-issues-recommendations-on-ai-says-regulatory-framework-for-development-of-responsible-ai-urgently-needed-11689859911432.html

Bailey, R., & Goyal, T. (2020, January 13). *Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2019*. The Leap Blog. https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html

Barik, S. (2024, July 13). Both Home and IT ministries pitch for control of nodal cyber security watchdog Cert-In. *The Indian Express.* https://indianexpress.com/article/india/both-home-and-it-ministries-pitch-for-control-of-nodal-cyber-security-watchdog-cert-in-9450203

Basu, A. (2025, May 13). *Data diplomacy: Rethinking cross-border data flows for a more equitable global digital economy*. Planetary Politics. https://www.newamerica.org/planetary-politics/blog/data-diplomacy-rethinking-cross-border-data-flows-for-a-more-equitable-global-digital-economy

Belli, L. (2023). Exploring the key AI sovereignty enablers (KASE) of Brazil, towards an AI sovereignty stack. Pre-print version. In Carnegie Endowment for International Peace (Ed.), *Digital Democracy Network Conference 2023 essay collection*. Buenos Aires. https://doi.org/10.2139/ssrn.4465501

Bhandari, V., & Rahman, F. (2020, May 25). *Constitutionalism during a crisis: The case of Aarogya Setu*. The Leap Blog. https://blog.theleapjournal.org/2020/05/constitutionalism-during-crisis-case-of.html

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLoS ONE*, *19*(4). https://doi.org/10.1371/journal.pone.0297312

BW Businessworld. (2025, January 30). IndiaAI Mission: Govt seeks proposals for foundational models, 18K GPU facility to debut soon. https://www.businessworld.in/article/indiaai-mission-govt-seeks-proposals-for-foundational-models-18k-gpu-facility-to-debut-soon-546497

Chandrasekhar, C., & Ghosh, J. (2021, August 23). The rising spectre of a telecom monopoly. *The Hindu Business Line.* https://www.thehindubusinessline.com/opinion/columns/c-p-chandrasekhar/the-rising-spectre-of-a-telecom-monopoly/article36063279.ece

CyberBRICS. (2024). *Digital public infrastructure for sovereign AI: A view from the BRICS* [Webinar]. https://cyberbrics.info/webinar-digital-public-infrastructure-for-sovereign-ai

Department of Science and Technology (DST). (n.d.). *25 Technology Innovation Hubs across the country through NM-ICPS are boosting new and emerging technologies to power national initiatives.* https://dst.gov.in/25-technology-innovation-hubs-across-country-through-nm-icps-are-boosting-new-and-emerging

ETTelecom. (2023, February 20). National Cybersecurity Strategy 2023 may come out soon: Pant. *The Economic Times.* https://telecom.economictimes.indiatimes.com/news/national-cybersecurity-strategy-2023-may-come-out-soon-pant/98093316

Indian Space Research Organisation (ISRO). (2023). *Indian Space Policy – 2023.* https://www.isro.gov.in/media_isro/pdf/IndianSpacePolicy2023.pdf

Jauhar, A. (2021). *Indian law enforcement's ongoing usage of automated facial recognition tech – ethical risks and legal challenges*. Vidhi Centre for Legal Policy. https://vidhilegalpolicy.in/wp-content/uploads/2021/08/210805_FRT_Paper1_Primer-Lit-Review_final.pdf

Kazia, N. A., Sinha, S., & Agarwal, S. (2025). *Consent managers: An Indian solution for managing consent.* International Bar Association. https://www.ibanet.org/consent-managers-Indian-solution

Kumar, D. (2024, July 1). Impact of Digital Competition Bill on India's homegrown startup ecosystem. *Business Standard.* https://www.business-standard.com/companies/start-ups/impact-of-digital-competition-bill-on-india-s-homegrown-startup-ecosystem-124070101008_1.html

Lenin, B. (2024). *India – Regulating software as medical devices – Navigating hurdles one byte at a time.* Conventus Law. https://conventuslaw.com/report/india-regulating-software-as-medical-devices-navigating-hurdles-one-byte-at-a-time

McDougal, L., Raj, A., & Singh, A. (2022, January 16). The digital divide and is it holding back women in India? *Hindustan Times.* https://www.hindustantimes.com/ht-insight/gender-equality/the-digital-divide-and-is-it-holding-back-women-in-india-101641971745195.html

Ministry of Communications. (2024). *Universal Connectivity and Digital India initiatives reaching all areas.* https://static.pib.gov.in/WriteReadData/specificdocs/documents/2024/aug/doc202486366801.pdf

Ministry of Electronics and Information Technology (MeitY). (n.d.). *FAQs.*

MeitY. (2023a). *IndiaAI 2023: Expert Group Report – First edition.* https://indiaai.gov.in/news/indiaai-2023-expert-group-report-first-edition

MeitY. (2023b). *Production Linked Incentive Scheme – PLI 2.0 for IT Hardware*. https://www.meity.gov.in/static/uploads/2024/02/Production-Linked-Scheme-2.0-for-IT-Hardware-notification_0.pdf

MeitY. (2024). *Due diligence by Intermediaries / Platforms under the Information Technology Act, 2000 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.* https://docs.google.com/document/d/1nc45Bqk2gU3GC9Say7rIB0xJuIfcd7jdjdHaMSrHXPs/mobilebasic

MeitY. (2025a). *Report on AI governance guidelines development*. https://indiaai.s3.ap-south-1.amazonaws.com/docs/subcommittee-report-dec26.pdf

MeitY. (2025b). *Request for proposal (RFP) for augmentation & enhancement of existing 8-inch fab of Semi-Conductor Laboratory (SCL), India.* https://www.meity.gov.in/static/uploads/2025/02/d60485e4181a949761bd4d4b6ab2799e.pdf

Mishra, A. (2024, July 4). Govt to use 50% of India AI mission funds for GPU procurement: MeitY. *Business Standard.* https://www.business-standard.com/technology/tech-news/govt-to-use-50-of-india-ai-mission-funds-for-gpu-procurement-meity-124070400728_1.html

Modi, N. [@narendramodi]. (2025, January 30). *When it comes to the space sector, bet on India!* [Post]. X. https://x.com/narendramodi/status/1884970434405535865

Mogul, R. (2023, March 1). India, world's largest democracy, leads global list of internet shutdowns. *CNN.* https://edition.cnn.com/2023/03/01/tech/internet-shutdowns-india-report-intl-hnk/index.html

Mohanty, A. & Sahu, S. (2024). *India's advance on AI regulation*. Carnegie India. https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en

Mostrous, A., White, J., & Cesareo, S. (2024). *The Global Artificial Intelligence Index.* Tortoise. https://www.tortoisemedia.com/2024/09/19/the-global-artificial-intelligence-index-2024

National Crime Records Bureau (NCRB). (2018–2023). *Crime in India.* Open Government Data (OGD) Platform India. https://www.data.gov.in/ministrydepartment/National%20Crime%20Records%20Bureau%20(NCRB)

NITI Aayog. (2018). *National Strategy for Artificial Intelligence: #AIforAll*. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

NITI Aayog. (2021a). *Responsible AI. #AIforAll. Approach Document for India: Part 1 – Principles for Responsible AI.* https://niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf

NITI Aayog. (2021b). *Responsible AI. #AIforAll. Approach Document for India: Part 2 - Operationalizing Principles for Responsible AI*. https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf

Pahwa, N. (2023, September 1). *How will India's Digital Personal Data Protection Law impact artificial intelligence?* [Video]. MediaNama*.* https://beta.medianama.com/2023/09/223-india-data-protection-law-impact-ai

Parsheera, S. (2022). Understanding state-level variations in India's digital transformation. *The African Journal of Information and Communication (AJIC)*, *30*, 1–9. https://doi.org/10.23962/ajic.i30.15082

Prasad, S. K. (2019). *Information fiduciaries and India's Data Protection Law*. Data Catalyst. https://datacatalyst.org/wp-content/uploads/2020/06/Information-Fiduciaries-and-Indias-Data-Protection-Law.pdf

Prime Minister of India. (2024, March 7). Cabinet approves ambitious IndiaAI mission to strengthen the AI innovation ecosystem. https://www.pmindia.gov.in/en/news_updates/cabinet-approves-ambitious-indiaai-mission-to-strengthen-the-ai-innovation-ecosystem

Republic of India. (2023). The Digital Personal Data Protection Act, 2023. https://egazette.gov.in/WriteReadData/2023/248045.pdf

Reserve Bank of India. (2018). *Storage of payment system data*. DPSS.CO.OD No.2785/06.08.005/2017-2018. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0

Saxena, P. (2021, June 11). *RAISE 2021 – Leveraging data for AI towards social empowerment*. IndiaAI. https://indiaai.gov.in/article/leveraging-data-for-ai-towards-social-empowerment

SEON. (2023). *Global cybercrime report: Which countries are most at risk in 2023?* https://seon.io/resources/global-cybercrime-report/ and https://assets.cdn.seon.io/uploads/2023/04/Cybersecurity_countries-min.pdf

Sheriff, K. (2020, December 14). NFHS data shows urban-rural, gender gaps in Internet use. *The Indian Express.* https://indianexpress.com/article/india/nfhs-data-shows-urban-rural-gender-gaps-in-internet-use-7103710

Singh, J. (2023a, January 25). *India's gig economy drivers face bust in the country's digital boom*. TechCrunch. https://techcrunch.com/2023/01/25/india-gig-workers-problems/?guccounter=1

Singh, M. (2023b, April 5). *India opts against AI regulation*. TechCrunch. https://techcrunch.com/2023/04/05/india-opts-against-ai-regulation

Singh, M. (2024, March 3). *India reverses AI stance, requires government approval for model launches*. TechCrunch. https://techcrunch.com/2024/03/03/india-reverses-ai-stance-requires-government-approval-for-model-launches

Singh, T., Shivraj, A., Madaan, S., & Nigam, M. (2025). *Unlocking AI's potential in India: Transforming agriculture and healthcare*. Boston Consulting Group. https://www.bcg.com/publications/2025/india-unlocking-ai-potential-in-india-transforming-agriculture-and-healthcare

Sur, A. (2024, July 1). *Digital India Bill likely to be delayed, government may opt for smaller, urgent regulations*. Money Control. https://www.moneycontrol.com/technology/digital-india-bill-likely-to-be-delayed-government-may-opt-for-smaller-urgent-regulations-article-12759435.html

Suraksha, P., & Lohchab, H. (2024, April 10). AI compute mission best served by marketplace model, say experts. *The Economic Times.* https://economictimes.indiatimes.com/tech/tech-bytes/marketplace-model-best-option-for-govt-to-offer-ai-compute-capacity-to-innovators-say-experts/articleshow/109169175.cms

Suri, A. (2025). *The missing pieces in India's AI puzzle: Talent, data, and R&D*. Carnegie India. https://carnegieendowment.org/research/2025/02/the-missing-pieces-in-indias-ai-puzzle-talent-data-and-randd?lang=en

Telecom Regulatory Authority of India (TRAI). (2023, June 19). *TRAI releases recommendations on 'Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India'* [Press release]. https://trai.gov.in/sites/default/files/2024-08/PR_No.54of2023.pdf

Varadarajan, L. (2025). Imperialism, the Third World and the fundamental continuities in Indian foreign policy. *Studies in Indian Politics*, *13*(1), 75–85. https://doi.org/10.1177/23210230251325599

Vipra, J. (2024). *A compute agenda for India*. Evam Law & Policy. https://cyberbrics.info/a-compute-agenda-for-india

Zwetsloot, R., Zhang, B., Anderljung, M., Horowitz, M., & Dafoe, A. (2021). *The immigration preferences of top AI researchers: New survey evidence.* Centre for the Governance of AI. https://www.governance.ai/research-paper/the-immigration-preferences-of-top-ai-researchers-new-survey-evidence