Prismatic Horizons
Journal of Social Science and Humanities
International Double-Blind Peer-Reviewed Referred Journal



Artificial Intelligence, Cybersecurity and Digital Governance: Evaluating Public Policy and Institutional Capacity in India

Aman Mishra[1] | **Khurshed Alam**[2]

[1] *Ph.D. Research Scholar in Political Science, Department of Humanities and Social Sciences, Integral University, Lucknow, Uttar Pradesh, India.*

[2] *Assistant Professor of Political Science, Department of Humanities and Social Sciences, Integral University, Lucknow, Uttar Pradesh, India.*

Email: amanji@student.iul.ac.in[1]

*** Corresponding Author:**

Aman Mishra

Email: amanji@student.iul.ac.in

ARTICLE INFO

Article History

Received	21 Jul, 2026
Revised	30 Aug, 2026
Accepted	25 Sep, 2026
Available Online	30 Sep, 2026

ARTICLE ID

PHJSSH0403002

KEYWORDS

Artificial intelligence policy, CERT-In, Cyber security governance, Digital governance, DPDP Act, India, Institutional capacity, India AI Mission.

ABSTRACT

Digital transformation has undergone considerable changes in India, specifically regarding public policy planning, over the past decade. The research aims to examine three connected entities: Artificial Intelligence Governance, Cybersecurity Governance, and Digital Governance Capacity in India. The research relies on the analysis of government documents, regulatory announcements, and a small number of studies of think-tanks and academia to analyze policy changes; in particular, the trends outlined in the NITI Aayog National Strategy for Artificial Intelligence in 2018 and related developments that paved the way for establishing the Indian AI Governance Guidelines and India AI Mission in 2024-2025, as well as the cybersecurity developments including the creation of CERT–IN and the National Critical Information Infrastructure Protection Centre and gradual implementation of the Digital Personal Data Protection Bill in 2023, among other issues. The findings demonstrate that, although the primary feature of Indian cybersecurity policy has a techno-legal, light regulation approaches, the processes outlined in this policy are rather limited because of existing deficiencies in the implementation. Although this approach has contributed to building a thick and more seasoned policy environment surrounding cyber and AI strategies, the most crucial barriers pertain to institutional capacity constraints, involving the absence of inter-agency synergies, uneven levels of expertise, and digital gap. According to the outcome of the analysis, the report gives proposals regarding coordination systems, regulatory abilities, and inclusiveness in the area of cybersecurity and digital governance.

OPEN ACCESS

JOURNAL INFO

ISSN: 2583-9284

Website: www.phjssh.lexarcheus.com

Vol. 04 | No. 03 | Jul-Sep, 2026 | Page: 10-22 | DOI: https://doi.org/10.5281/zenodo.23021347

How to Cite This Article

Aman Mishra, Khurshed Alam, "Artificial Intelligence, Cybersecurity and Digital Governance: Evaluating Public Policy and Institutional Capacity in India," *Prismatic Horizons: Journal of Social Science and Humanities*, vol. 4, no. 3, 2026, pp. 10–22.

© 2026 The Authors, Published by (PHJSSH). This is an Open Access Article under the Creative Commons Attribution 4.0 International (CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/)

1. INTRODUCTION

India has an important role in the digital space. Firstly, India is considered as the second highest populous country after China and is also the second highest Internet populated country. Secondly, India is now emerging as a major player in the digital world and is getting louder in terms of establishing the rules around digital technology. Thus, the importance of India's digital presence can be substantiated by the fact that Government of India claims that the number of Internet subscribers crossed the 1-billion mark by 2025. It is to be noted that this number was just about Rs. 251 million as in March 2014 (Press Information Bureau, 2026). Much of this has been fueled by the Digital Public Infrastructure stack developed by the Indian Government such as Aadhaar, Unified Payments Interface (UPI), and DigiLocker, which is also considered the basis of various applications for both private and public sectors (National e-Governance Division, 2025). Although technological advancement is increasing, the risks and threats are also increasing such as data breach as well as financial fraud. The Government of India has already started developing a policy framework consisting of artificial intelligence strategy, cyber security action plan, and data protection law in order to protect the digital space of India.

The paper looks at three different but related topics: AI governance, cybersecurity and data protection looking at how well the authorities in charge of implementing them are set up, coordinated and given authority to do their work.

The rest of the paper is structured as follows. In Section 2, I will review the literature available on AI governance, cybersecurity governance, data protection and institutional capacity. In Section 3, I will elaborate on the methods used in this research. Section 4 presents a model for assessing capacity in the area of digital governance. Section 5 discusses the evolution of India's AI policy, from the 2018 National Strategy for Artificial Intelligence to the 2025 AI Governance Guidelines. Section 6 presents the cybersecurity governance system that is based on CERT-In's and NCIIPC's work. Section 7 presents the Digital Personal Data Protection Act, 2023, and its 2025 Rules, which represent the link between the two areas mentioned above. In Section 8, I will identify the gaps in the institutional capacity. Section 9 presents the outcome of the findings of this analysis, and Section 10 presents the results. Section 11 explains the importance of the results in practical terms, while Section 12 provides the practical recommendations on how to put knowledge to work. Finally, Section 13 wraps up the discussion.

The study is also relevant to the Sustainable Development Goals (SDGs), particularly SDG 8 "Decent Work and Economic Growth", SDG 9 "Industry, Innovation and Infrastructure", and SDG 17 "Partnerships for the Goals". SDG 8 promotes productive employment, decent work, entrepreneurship, technological upgrading and innovation as components of sustainable economic growth (United Nations, 2015a). In the context of AI and digital transformation, these dimensions are important for developing new skills, improving productivity and creating technology-driven economic opportunities. SDG 9 focuses on resilient infrastructure, inclusive industrialisation and innovation, highlighting the importance of technological capabilities and digital infrastructure for development (United Nations, 2015b). India's IndiaAI Mission similarly seeks to develop AI infrastructure, datasets, foundation models, future skills and innovation capacity (Ministry of Electronics and Information Technology, 2024). Furthermore, SDG 17 emphasises global cooperation and multi-stakeholder partnerships involving governments, the private sector, civil society and other stakeholders (United Nations, 2015c). Therefore, the present study connects AI governance, cybersecurity and digital governance with broader objectives of economic growth, technological innovation, digital infrastructure and institutional partnerships.

Statement of the Problem

In the last decade, India has taken on an ambitious digital governance agenda with the implementation of an Artificial Intelligence strategy, cybersecurity institutions and a system of data protection. However, the emergence of the new policies has revealed the gap between what has been set by the guidelines and the capacity that regulators have in order to put forward policies. The introduction of the India AI Governance Guidelines has shown this capacity issue enshrined in the documents, while CERT-In's report indicates the increasing amount of cyber threats and the personnel engaged in resolving them. The phased implementation of the Digital Personal Data Protection Act indicates the problem with institutional capacities necessary for enforcement of the law. Thus, the aim of this report is not to analyze whether India has developed any new

digital policies but whether the existing institutional system is capable of implementing these new developments, as the response may have the character of a wish.

Objectives of the Study

The scope of the research entails the following objectives:

1. To appreciate the historical development of the Artificial Intelligence policy of India, starting with the 2018 National Strategy for Artificial Intelligence and culminating with the 2024 IndiaAI Mission and the 2025 India AI Governance Guidelines.
2. To explore the institutional framework of cybersecurity governance in India, from CERT-In, NCIIPC and the National Cyber Security Coordinator to the Indian Cyber Crime Coordination Centre.
3. To analyze the Digital Personal Data Protection Act, 2023 and its 2025 Rules as a unifying regulatory framework which will help establish relationships between AI governance and cyber security governance.
4. To ascertain the capacities and gaps in structural aspects, such as coordination among agencies, human resources and technical capabilities, clarity of enforcement and inclusivity in terms of digitalization.
5. To explain whether India's approach toward regulation is based on important underlying realities or it just happens to favor the light touch regulatory regime.
6. To recommend evidence-based suggestions for enhancing coordination mechanisms, regulatory capacities and inclusive digital governance in India.

Scope of the Study

The study is limited to a national approach to digital governance in India and does not consider issues at a state or sector level. The focus is on three aspects of digital governance: (i) AI policy which includes a national strategy and plans for implementation, (ii) cybersecurity governance which includes regulatory agencies, and (iii) data protection law dealing with the DPDP Act and its implementation rules. The time frame included ranges from 2018 when the National Strategy for AI was published to 2026 with reference to developments such as the IndiaAI Mission, the AI Governance Guidelines, and the DPDP Rules. The information used comes from government publications, communication materials, and reports or comments from law companies.

Significance of the Study

The importance of this research resides in its timing and methodology. As the IndiaAI Mission and its AI Governance Guidelines and DPDP Rules are set to be put into practice in 2024-2025, the fact that this research does not cover these issues separately, but also puts together these developments, is crucially important, especially for policymakers who can benefit from the value of this study while creating new reforms. For the researchers and students of public policy and governance, it offers a uniquely positioned case study of how a large democracy with limited resources aspires to cope with fast-evolving technologies through institutional change. For people engaged in the business and civil society sphere, the research is of interest since it indicates what functions belong to the relevant institution and what missing links exist in implementation and accountability mechanisms.

Literature Review

There are four major streams within the literature that is relevant to this study: writings on Artificial Intelligence governance and regulation; writings on cybersecurity governance and institutional structure; writings on data protection and privacy law; and the general public administration literature about the state and institutional capacity. All of these streams will be dealt with briefly below, after which the gap that this study intends to fill will be pointed out.

Literature on Artificial Intelligence Governance

NITI Aayog's National Strategy for Artificial Intelligence (2018), India's first-of-its-kind document on AI, emphasizes the relevance of this technology in terms of being an instrument for inclusive development

rather than in profit-making or defense-related terms. Practitioners' writings on IndiaAI Mission and the India AI Governance Guidelines 2025, predominantly authored by law and consulting firms instead of academic scholars, repeatedly mention that India has chosen "soft law" models based on principles rather than strict legal regulations as practiced by the EU in AI governance. Such literature mainly provides insight into the institutional architecture behind the AI Governance Group, Technology Policy and Expertise Committee, and AI Safety Institute but not much about the adequacy of staffing or resourcing of these institutions.

Literature on Cybersecurity Governance

A parallel literature maps out the statutory and institutional architecture built around the Information Technology Act, 2000, especially CERT-In and the National Critical Information Infrastructure Protection Centre (Carnegie Endowment for International Peace, 2025). The literature contains a wealth of quantitative information on the scale of CERT-In's operations, such as annual incident volumes and training outputs, based largely on official government reporting (Press Information Bureau, 2026a; Vision IAS, 2026). Complementary industry commentary provides context to the development of India's cybersecurity policy from the National Cyber Security Policy of 2013 to the anticipated new National Cyber Security Strategy, and generally agrees that institutional proliferation, that is, the addition of new coordinating bodies over time, has outpaced the development of a single, authoritative coordination mechanism (Mind of Cyber, 2025; RSM India, 2025).

Literature on Data Protection and Privacy

The conversation around the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 has largely been about legal assessment for compliance driven businesses, phased roll-out schedule and the SARAL drafting methodology employed by the Ministry of Electronics and Information Technology (Lexology, 2025; IAPP, 2025; DLA Piper, n.d.). Some of this literature raises interpretive questions as to the extent to which the consent and purpose limitation provisions of the Act would apply to data used to train AI models and suggests that regulatory clarification, rather than new legislation, is the more likely course of action in the immediate term (Khaitan & Co./ERGO, 2025).

Literature on State and Institutional Capacity

In addition to the literature on India, public administration scholarship offers a useful lexicon for the present study. Fukuyama (2004) distinguishes between the breadth of state functions, the scope of activities a government undertakes and the strength or ability of state institutions to carry out those functions effectively. Fukuyama argues that often governance problems arise from a mismatch between the two. Similarly Grindle (2004) cautions against the assumption of comprehensive, 'best practice' institutional design being sufficient in resource-constrained contexts, arguing for a 'good enough governance' approach that focuses on the capacities most critical to a particular policy issue.These frameworks are relevant to India's digital governance experience, where the ambit of policy ambition, covering AI, cybersecurity and data protection has expanded rapidly and the underlying institutional strength is still evolving, by the government's own admission.

Research Gap

The existing literature has rich descriptive details on India's AI, cybersecurity and data protection frameworks, but individually, largely from a legal-compliance or journalistic lens, rather than from an institutional-capacity lens. Few studies examine the three domains collectively as a single digital governance system, and fewer still use a specific policy-institutions-capacity framework to evaluate the extent to which India's institutional architecture corresponds to its policy objectives. This study aims to bridge this gap by integrating all three domains into a coherent analytical framework and by systematically identifying the capacity constraints that exist in all three.

Research Methodology

Research Design

The study utilizes an approach of qualitative, doctrinal and analytical research that fits well for policy and institutional analysis of this nature. The study is conducted using a single-country embedded case study design where India is treated as the overall case whereas the three areas of governance – Artificial Intelligence,

cybersecurity and data protection, are treated as the embedded units of analysis that are looked into separately but analyzed collectively in the discussion. It is essentially a descriptive-analytical design rather than experimental and hypothesis-testing since the existing policy and institutional framework will be described first based on official documentation and other sources of secondary material, after which the same framework will be analyzed in light of the theoretical framework provided in Section 4. Since the research is conducted entirely through documentation, it may better be classified as qualitative review and analysis paper.

Data Collection Methods

The data for the analysis have been sourced entirely from secondary sources through a purposeful documentary research approach. The primary government sources, which include the National Strategy for Artificial Intelligence (2018) of the NITI Aayog, India AI Governance Guidelines (2025), Press Information Bureau communications, the yearly reporting of CERT-In and the Digital Personal Data Protection Act, 2023 and its Rules of 2025, have been taken as the core data source. Additionally, the secondary sources from well-known law firms, policy advisory firms, think-tanks, and news portals such as Carnegie Endowment for International Peace, Atlantic Council, Vision IAS and Chambers and Partners have been considered secondary sources that have been utilised mainly to provide an interpretation of the core data sources rather than an independent source of facts. Selection criteria of sources have been based on relevance to the three governance dimensions, recency prioritising publications made within 2023 to early 2026 – and, in the case of the secondary sources, the credibility of the publication institution.

Data Analysis Techniques

Being that this research paper is a documentary and review based study and not an empirical research based on a survey or interviews, the sample population was not needed since the unit of analysis in this case is not made up of human beings but a collection of policy, legal and institutional documents obtained in the process of data collection as described above. However, in some cases, where population and sample population issues came into consideration, for example the population sizes of internet users, cybersecurity experts, and informal sector workers mentioned in section eight of this report, these figures have been taken straight from the government and industry sources cited in this research paper. Qualitative content analysis and thematic analysis were used in analyzing the data obtained. The documents were analyzed manually based on the three dimensions of the theoretical framework which include policy design, institutional arrangement, and operational capability, as well as four emerging themes which include inter-agency coordination, human capital and technical expertise, legal clarity and enforcement, and digital inclusion. A version of comparative policy analysis was also employed in Section 6 and 11, placing India's policy decision making, in particular its use of soft law and sectoral regulation, in contrast with the prescriptive nature of the EU's AI Act and the voluntariness characteristic of policies in the United States, to understand the importance of India's institutional design decisions.

Conceptual Framework: Policy, Institutions and Capacity

Three factors regarding digital governance capacity should be considered: Policies, which are influenced by the guidelines and rules that should be clear, consistent and relevant; Institutional Architecture which is influenced by agencies, coordination instruments and legal instruments used to implement policies; and Operational Capacity which consists of personnel, technology and funds available to the institution to carry out its mission.

However good a policy may be, it can fail in its implementation if the agency that implements it does not have enough trained personnel, does not have an instrument for dividing authority among competing agencies, or has no means of enforcing it. It is true especially in India where the capacity problem is recognized as an important one in specific policy documents related to AI and cybersecurity (Ministry of Electronics and Information Technology, 2025a).

Another useful differentiation shown by regulatory comparisons is the differentiation between hard law and soft law. Hard law is binding law while soft law is voluntary. At the present time, the regulatory framework of India regarding AI uses much soft law because of the lack of regulatory capacity and fast changes in the field (Sai Krishna & Associates, 2025).The way in which the Indian government has opted to regulate AI cannot simply be seen in terms of philosophy alone as an answer to the problem at hand, but as just one of

several ways of dealing with constraints to the abilities of the government, which are discussed in later sections of this essay.

India's Artificial Intelligence Policy Landscape

From the National Strategy for AI to the India AI Mission

The official involvement of India in AI policy started with the National Strategy for Artificial Intelligence by NITI Aayog titled "AI for All" published in June 2018. The five focus sectors for the use of AI were identified as healthcare, agriculture, education, smart cities & infrastructure, and smart mobility, with AI being seen as a tool for achieving inclusive growth as opposed to its being a mere commercial tool (NITI Aayog, 2018). The concept of using AI as a development tool is one of the cornerstones of Indian AI policy which distinguishes India from the US and China alike (Atlantic Council, 2025).

The strategic vision outlined above became a reality about six years down the line, when the Union Cabinet gave approval to the IndiaAI Mission, which took off on March 7, 2024 with a budget of approximately ₹10,371.92 crore (approximately $1.25 billion for five years). The mission is executed through the Independent Business Division of IndiaAI under the Digital India Corporation under the aegis of the Ministry of Electronics & Information Technology (MeitY) through seven pillars that include computing infrastructure, indigenous foundation model, datasets platform (AIKosh), applications, skilling, start-ups financing and "Safe and Trusted AI" (PIB, 2025b). According to reports from the Mission, towards the end of 2025, there had been scaling from an initial aim of 10,000 GPUs to about 38,000 GPUs with the AIKosh Platform integrating more than 5,500 datasets and more than 250 AI models across twenty sectors (PIB, 2025b). Twelve start-ups, which included Sarvam AI and the consortium of BharatGen from IIT Bombay, were given contracts under the Sovereign Model Pillar of the mission for developing indigenous large multimodal models.

This need for infrastructure is based on an assumption, found implicitly in various policy documents from India, that the main problem in developing AI is not one of ambition but rather that of capacity regarding computing power, curated data, and labor force. The Mission has focused especially on creating availability of affordable GPU services through a market-based approach, as well as multilingual abilities through the Bhashini project, to help overcome the difficulties related to India's substantial population of non-English speaking people, who have traditionally had little access to technologies in their own languages (NeGD, 2025).

The India AI Governance Guidelines, 2025

Issued on November 5, 2025 by MeITy, AI Governance Guidelines comprise the first national dedicated regulatory framework to govern artificial intelligence. The AI Governance guidelines describe it in the dual capacity of technology and law in a techno-legal approach in which it states that much of the current law is sufficient to deal with any conceivable harm of AI in future while there may be limited adjustments to determine how AI-based developers, deployers, users would classify the harmful actions and who to allocate blame. For the drafting of AI Governance Guidelines, a committee proposed seven principles in the name of 'sutras' as Trust; people-first design; innovation rather than stifling it; fairness and equality; accountability; understandable by design; and safety, sustainability and resilient, principles mirroring several features in theRBI's Framework for responsible and Ethical Enablement of AI (Sai Krishna & Associates, 2025).

It defines AI governance as involving both technology and law, following a techno-legal framework that assumes that existing laws already cover most foreseeable AI-related harms, while only certain targeted amendments are necessary to clarify how to categorize and attribute liability for developers, users and deployers of AI (Sai Krishna & Associates, 2025).

The institutional framework includes an entirely new whole-of-government structure with three new institutions: An AI Governance Group (AIGG), comprised of several government departments that will oversee and support the AI, presided over by the Principal Scientific Adviser's appointee to coordinate all AI efforts within the government and advocate for the responsible adoption of AI; A Technology Policy and Expertise Committee (TPEC) to assist all government bodies with technical and legal guidance related to AI; and An AI Safety Institute (AISI) to manage AI testing, risk assessment and AI international partnerships (Chambers & Partners, 2025). Meanwhile, existing sectoral bodies, such as the RBI, the Securities and Exchange Board of India, and the Telecommunications Regulation Authority of India are to maintain their

regulatory authority and to carry out enforcement within their sectors, with MeITy designated as the leading ministry for coordination. Capacity was also listed as a risk factor, highlighting the limits faced by regulators and the authorities in governing AI and the need for training to avoid overburdening SMEs and other entities at the forefront of AI adoption (Insights on India, 2025). This acknowledgment from Indian policymakers suggests that the current institutional infrastructure that is to be put in place to govern AI will outstrip human resources.

Cybersecurity Governance in India

Legal Foundations and CERT-In

India's legal foundation is anchored in its cybersecurity legislation, with most policy provisions contained in the IT Act, 2000, as amended over time, serving as the legislative framework enabling national cyber responses. As mandated by Section 70B of the IT Act, CERT-In functions as India's premier cybersecurity agency, collating and examining information on computer security incident events and sharing the collected information (Carnegie Endowment for International Peace, 2025). CERT-In further directed all companies, in a 2022 update to the IT Act under Section 70B, to notify cyber events within six hours of occurrence, a much quicker timescale than many other nations. CERT-In has achieved a formidable operational reach. According to data released from governmental sources, CERT-In reported responses to 29,44,777 (almost 3 million) cyber incidents over the year 2025 and issued 1,530 security alerts, 390 vulnerability notes, and 65 advisories (PIB, 2026a; Vision IAS, 2026). Along with the collection and processing of cyber-incident data, CERT-In supports a number of cybersecurity activities. This include its "Cyber Swachhta Kendra," which is involved with botnet and malware analysis and cleanup to promote good cyber hygiene among Indian residents, and the "National Cyber Coordination Centre," a real-time awareness platform that oversees a wide array of cybersecurity-related activities, including sector-specific CSIRT bodies like "CSIRT-Fin" for financial entities and a national "Cyber Crisis Management Plan" to manage large-scale security attacks. During 2025, the organization had registered more than 231 companies that offer a full spectrum of certified security audits, educated over 21,000 people in police forces and cybersecurity, and organized a total of 122 cybersecurity drills with the participation of approximately 1,570 organizations across the defence sector, telecommunications, energy, and financial sector (PIB, 2026a).

Institutional Architecture: NCIIPC, NCSC, and I4C

Another body that is responsible for supporting CERT-In is the National Critical Information Infrastructure Protection Centre (NCIIPC), which was established under section 70A of the IT Act in order to safeguard the 'critical information infrastructure', which means "systems whose incapacity could impair national security, the economy, public health and safety" (Carnegie Endowment for International Peace, 2025). The institution prioritised six 'sectors': banking and finance, power and energy, telecommunications, transport, healthcare, and strategic public enterprises, issuing a sector-specific advisory on vulnerabilities of networked medical devices in February 2025 (Carnegie Endowment for International Peace, 2025).

The body forms the peak of the hierarchy when it comes to the coordination of activities because it coordinates CERT-In, NCIIPC, Ministry of Electronics and IT (MeitY), Ministry of Home Affairs, Department of Telecommunications and Ministry of Defence Research and Development Organization (Carnegie Endowment for International Peace, 2025). The enforcement co-ordination (distinct from the technical incident response) is the job of Indian Cybercrime Co-ordination Centre (I4C) under Ministry of Home Affairs, which is responsible for the National Cyber Crime Reporting Portal as well as the '1930' telephone number for financial frauds (Vision IAS, 2026).

It can therefore be concluded that the governance structure for cybersecurity in India has various layers, whereby agencies collaborate through two major pathways, one based on national security and the PMO, while the second one is based on the MeitY. Although having layers helps in having redundant and specialized agencies, it leads to duplication and lack of coordination between the two pathways, as seen in Section 8 below.

Policy Evolution: From the 2013 Policy to a New National Strategy

The National Cyber Security Policy of 2013 is regarded as India's first ever comprehensive cybersecurity policy which has outlined certain fundamental objectives that still form the basis of present-day practices like building a safe cyberspace environment, ensuring the protection of critical infrastructures, promoting cybersecurity research and development, and public-private partnerships. Though being outdated today, the 2013 Policy has provided an excellent institutional framework, namely the establishment of NCIIPC and capacity building measures like Information Security Education & Awareness (ISEA) (Mind of Cyber, 2025). At the moment, the National Security Council Secretariat is working on the new National Cyber Security Strategy to replace the 2013 Policy, with the latter likely to address such challenges as supply chain/application security, AI-based threats, and cybersecurity threats linked to large-scale digitalization of public services (Mind of Cyber, 2025; RSM India, 2025).

Data Protection as the Connective Layer: The DPDP Act and Rules

The Digital Personal Data Protection Act, 2023 (DPDP Act) forms the legal basis that links AI governance and cybersecurity policies, in that they are both about the proper use of personal information. The DPDP Act got assent from the President on 11 August 2023 and came after the 2017 ruling of the Supreme Court in the case of Justice K. S. Puttaswamy (Retd.) v. Union of India, where it was ruled that privacy is a fundamental right under Article 21 of the Indian constitution, thus making way for a separate data protection law.

Approval by the Ministry of Electronics & IT (MeitY) of the Digital Personal Data Protection Rules, 2025 on 13 November 2025, together with the formation of the Data Protection Board of India, which will have four members, forms a phased-in schedule to implement the provisions of the Act. The administrative provisions and the formation of the Data Protection Board of India become effective immediately; registration of consent managers, intermediaries to help the individual manage datasharing consents, becomes effective one year after notification; while the substantive provisions become effective in May 2027 (Lexology, 2025; PIB, 2025d). SARAL (Simple, Accessible, Rational, and Actionable) is the government's declared philosophy of drafting, which aimed at lowering compliance costs for small companies (PIB, 2025d).

There still seems to be some ambiguity surrounding the issue of AI governance under the DPDP regime. Among the open issues include the treatment of consent-based processing of scraped/aggregated data for training large models, applicability of correction/erasure rights to original data that was part of a trained model, and applicability of the principle of purpose limitation when using data collected for one purpose for training other models (ERGO/Khaitan & Co., 2025). Such ambiguities are one of the main reasons why Indian regulators decided to "wait and clarify" before drafting specific data laws for AI.

Institutional Capacity: Achievements and Structural Gaps

Coordination and Fragmentation

There are many agencies involved in India's digital governance framework, such as MeitY, CERT-In, NCIIPC, NCSC, I4C, sectoral regulators, and, relatively recently, AI Governance Group (AIGG), TPEC, and AISI. Every one of these agencies has its own mandate, though there is overlap between mandates of some agencies. This approach ensures specialisation and makes it impossible for the whole digital governance system to break down. Still, the Guidelines on AI Governance as well as numerous evaluations from outside indicate that the distribution of responsibilities between the agencies is quite loose and can be significantly improved in terms of better cooperation. A more solid coordination mechanism would help to create some consistency in the implementation of the national strategy and risk assessment and implementation process (PIB, 2025a). The combination of the security-focused NSCS coordination approach and technology-focused MeitY coordination approach serves as evidence of the necessity of the bridging.

Human Capital and Technical Capacity

Institution design requires individuals who are effectively recruited, staffed and trained. Reporting from CERT-In highlights an important commitment to the matter, having designed 32 special training programmes related to technology, benefiting more than 91,000 individuals through 95 awareness campaigns and training about 21,000 officers until 2025 (PIB, 2026a). It demonstrates substantial investments, but the challenge behind the problem is enormous, millions of cyber incidents take place every year and the shortage

of cybersecurity specialists (estimated at 650,000) prevents India from tackling cybercrime (Vision IAS, 2026). Finally, the need for "regulator and law enforcement agency training", highlighted by the AI Governance Guidelines, shows that the technical literacy needed to evaluate AI-related problems (algorithmic bias, algorithmic opacity, and synthetic media manipulation) is deficient in most regulatory bodies (Insights on India, 2025).

Enforcement, Sectoral Regulation, and Legal Ambiguity

In choosing regulation of AI based on existing sectoral regulators, the regulator can make use of its existing domain expertise. At the same time, the approach will result in inconsistencies in the standards applied from sector to sector as the regulator will have different interpretations of the ideas of fairness, explainability, and accountability.

Several legal uncertainties persist due to the lack of adequate institutions to resolve them, namely, how the concepts of 'intermediary' and 'publisher' under the Information Technology Act relate to AI developers and deployers, who is liable in the case of harm caused by an autonomous AI, and whether safe harbor provisions for passive intermediaries can be extended to generative AI systems which create content. As long as the uncertainties are not resolved, enforcement of regulations is unlikely to be consistent.

The Digital Divide and Inclusion

Inclusion of different stakeholders is yet another aspect of capacity. The report on AI for Inclusive Societal Development by NITI Aayog (October 2025) defines the key policy issue as "how to ensure that AI and IoT and associated technologies reach instead of bypass the roughly 490 million Indians working in the informal economy" (PIB, 2025b). Institutional capacity of digital governance is relevant as long as citizens have the capability to use, understand and enforce their rights under the framework set out in DPDP Act. Digital literacy is not uniformly prevalent in India's socio-cultural and geographic segments, leading to discrepancies in terms of languages and connectivity in tier-1 cities as compared to smaller towns, making it difficult for citizens to enforce the rights that have been conferred upon them by law.

Findings of the Study

The following key observations have been made through the documentary analysis undertaken in Sections 4 to 8:

Infrastructure development outpaces the development of human capacity. While the IndiaAI Mission has significantly surpassed its own benchmarks concerning computing capacity infrastructure – scaling up from an intended 10,000 GPUs to almost 38,000 GPUs along with onboarding of more than 5,500 datasets on the AIKosh platform by 2025 (PIB, 2025b), there has been no indication of such an explosion in the size of the specialized workforce required for the audit of AI regulation.

The approach of soft law is determined by capacity limitations, not only ideology. AI Governance Guidelines, 2025 is built largely upon the existing law and voluntary principles and not an AI statute, which is explicitly attributed to capacity limitations and the pace of technological development by official Indian sources (Sai Krishna & Associates, 2025; Ministry of Electronics and Information Technology, 2025a). This means that the "light-touch" approach of India was chosen primarily due to capacity considerations.

Cybersecurity architecture is operationally dense but layered structurally. The handling of over 29 lakh incidents by CERT-In in 2025, in combination with NCIIPC's critical infrastructure responsibility and the multi-agency coordination role of the National Cyber Security Coordinator, indicates significant operational activity, but the coexistence of a security-oriented (NSCS) and technology-oriented (MeitY) coordination pathway raises the risk of duplication at their interface (Carnegie Endowment for International Peace, 2025).

The DPDP Act is a connective but incomplete regulatory layer. The connection between AI governance and cybersecurity governance is achieved in the Digital Personal Data Protection Act, 2023, and its 2025 rules by virtue of common data-protection obligations, but there are unresolved issues surrounding consent for AI training data, correction and erasure rights in trained models, and limitations of purpose of repurposed data, which the phased implementation does not resolve (ERGO/Khaitan & Co., 2025).

India's policy documents are remarkably self-critical about capacity. Unlike many other comparative regulatory documents, India's own AI Governance Guidelines and other official documents recognize the possibility of insufficiency of regulatory and enforcement capacity compared to the breadth of the mandate, particularly among micro, small and medium enterprises as AI deployers (Insights on India, 2025).

Human capital investments are significant in their own right but small in proportion to their scale. Training of approximately 21,000 officers and 91,000 awareness-programme participants by CERT-In is a significant institutional investment; however, it is small compared to India's internet user base that has now exceeded one billion connections and also the Indian cybersecurity workforce that has been described as inadequate to meet current needs (Vision IAS, 2026).

Fragmentation of regulation by sectors raises concerns about inconsistent application. Since AI regulations are fragmented and regulated by sectoral regulators like the Reserve Bank of India, the Securities and Exchange Board of India, and the Telecom Regulatory Authority of India, the definition of fairness, accountability, and similar aspects will vary among sectors. Thus, an underlying risk associated with AI may receive different treatment from different sectoral regulators.

As far as digital inclusion is concerned, it continues to be an afterthought, rather than being part of the core focus of the designs. While there have been discussions about India having about 490 million informal workers in NITI Aayog's report on AI for inclusive societal development, and while there have also been multilingual programs like Bhashini, the capacity building discussed in the official reports has been done for the regulators and enforcing agencies instead of for digital literacy of the citizens.

Data Analysis and Interpretation

Interpreting the results in Section 9 from the policy-institutions-capacity perspective described in Section 4, along with the four thematic categories generated during the data analysis process, this section presents an interpretation of the results from an interpretative perspective, based on the findings' meaning for India's digital governance model.

Theme One: Capacity Constraints Shape Policy Choice

In this regard, the case analysis in sections 5 and 6 shows that it would be more realistic to consider India's prioritisation of investments in institutions and infrastructure over legislation to be an appropriate and pragmatic approach within the limitations of capacity. While according to Fukuyama (2004), governance issues emerge when there is an imbalance between the ambitions of the state and its institutions, the Indian approach towards digital governance seems to be an effort at addressing this imbalance not by strengthening the institutions but rather by augmenting the number of institutions and infrastructure required for this scope, such as AI Governance Group and AI Safety Institute and GPU capacity and AIKosh, respectively. In this way, the approach taken by India conforms to the "good enough governance" logic proposed by Grindle (2004).

Theme Two: Coordination Architecture is necessary but not Sufficient

The overlapping cybersecurity and AI coordination mechanisms mentioned in Sections 6 and 8.1, including CERT-In, NCIIPC, the NCSC, I4C, the AI Governance Group, and the Technology Policy and Expertise Committee, add redundancy and specialization, which is a true institutional advantage. But based on the analysis, the fact that there are parallel coordination channels – one focused on security issues and operating from the Prime Minister's Office, the other one focused on technology issues and operating from MeitY – is precisely what makes coordination difficult and becomes part of the problem identified in government documents. Having more coordinating entities does not replace the need for the responsible entity to be identified.

Theme Three: Legal Clarity Is Being Deferred, Not Resolved

In both the AI Governance Guidelines and the DPDP Rules, what we see again and again is deferral – the deferral of issues regarding liability of autonomous AI systems, the application of safe harbor to generative AI, and the use of AI training data within data protection law. From the capacity perspective, it is perhaps not surprising that these issues are deferral; solving them would in itself be a matter that would require capacity

beyond what the documents recognize as having been developed at this point. What the analysis also suggests is that there is a danger in the deferred approach, insofar as deferral may lead to inconsistent enforcement, as each regulator court interprets ambiguous provisions differently.

Theme Four: Inclusion Remains Structurally Secondary

Third, the findings discussed in Sections 8.4 and 9 also show that although digital inclusion is mentioned explicitly in certain documents, like the NITI Aayog's report on AI and inclusive societal development, it has not become part of the core capacity-building framework to the extent that the need for training regulators and building technical infrastructure have. In fact, most capacity-building activities discussed in this study seem to be aimed at building up the capacities of the institutions themselves and not their ability to guarantee citizens' access to their rights. This imbalance may mean that even the most well-trained regulatory system would still fail to deliver benefits to a significant part of India's population.

All in all, the four main themes discussed in this study lead to one conclusion, that the Indian digital governance framework can only be seen as an experiment with various institutions that lack necessary capacities to address digital security threats efficiently.

Discussion: A Distinctive but Strained Model

India's strategy towards AI, cybersecurity, and data governance is guided by a common basic principle: create institutions and infrastructure first, regulation should be light-handed and adaptive, and where legislation is required it should be reactive not preemptive. These efforts yielded concrete results, namely, increased infrastructure development, implemented within the framework of the IndiaAI Mission; an operational national emergency response system managed by CERT-In, which annually deals with millions of incident reports; and a data protection act which although its implementation takes longer than planned still follows well-proven principles of data governance internationally recognized as the rules of consent, limitations of usage, and accountability. Contrasting the EU prescriptive and risk-oriented AI Act, India's approach is much more based on the institutional judgment and expertise of sectors and similar to the approaches of innovation-led governance characteristic of Japan and the USA (Chambers and Partners, 2025).

The approach is therefore inevitably a gamble as well since a light-handed regulation that relies on capacity can be only as effective as the very same capacity itself. The policy documents of India are quite transparent about the present state of the above-mentioned systems where many problems including those related to coordination, capacity building, and legal clarification remain unresolved (Press Information Bureau, 2025a).

What will be a key challenge for the Indian government during the next few years would be implementation. Is there enough capacity within the AI Governance Group to implement its mandate? Would CERT-In and NCIIPC create the capacity required to effectively deal with an increasingly challenging environment? Would the Data Protection Board of India be able to establish its adjudicatory capacity to handle an increased number of complaints under the DPDP Act in 2027?

Policy Recommendations

Following the analysis outlined above, this paper recommends five measures. First, institutionalise cross-agency coordination and confer clear authority by giving the convening powers for either the AI Governance Group or the National Cyber Security Coordinator's office so as to resolve any ambiguities regarding jurisdiction before they become contentious. Second, allocate funds to recruit specialist regulatory personnel by giving sectoral regulators and law enforcement agencies the resources to train their officers in skills such as model auditing, digital forensics, and cryptographic security, possibly in dedicated career paths in the civil service instead of workshops. Third, address legal ambiguities proactively by working on targeted amendments that clarify the classification of developers, deployers, and users of AI and their liability under the IT Act instead of leaving them for interpretation in the slow process of case law. Fourth, anticipate adjudicatory needs and act accordingly by ensuring the Data Protection Board of India is sufficiently staffed and equipped digitally before May 2027 when the substantive parts of the DPDP Act come into force because of the number of complaints likely to come from over one billion internet users in the country. Fifth, incorporate the metric of inclusion within capacity analysis; institutions should not just measure the number

of cases processed or guidelines produced, but how inclusive their mechanisms for redress and grievances are to those with poor digital literacy skills.

Conclusion

Currently, India is constructing a robust digital governance regime that depends on an infrastructure-based model and institutional coordination rather than on prior legislation. The establishment of the IndiaAI Mission and 2025 AI Governance Guidelines, the presence of a matured CERT-In led cybersecurity regime, and a near-completed Digital Personal Data Protection Act, India is in possession of what can be described as one of the most developed digital governance regimes among developing countries. However, this regime will stay incomplete until the public institutions that will have to implement it become sufficiently mature according to the schedule outlined by the Government of India. In order to turn India's digital governance agenda into action, continuous investment into coordination, regulatory personnel, and adjudication infrastructure will be needed.

Acknowledgement

I Aman Mishra, Research Scholar (Enrollment number 2400105943) of Integral University Lucknow has prepared this research paper the University has provided me Manuscript communication number IU/R&D/2026-MCN0005062. In the future I will keep on working on improving my research work as per the standards.

REFERENCES

Atlantic Council. "India's Path to AI Autonomy." *Atlantic Council*, 13 Mar. 2025, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/indias-path-to-ai-autonomy/.

Carnegie Endowment for International Peace. "Mapping India's Cybersecurity Administration in 2025." *Carnegie Endowment for International Peace*, Sept. 2025, https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025.

Chambers and Partners. "MeitY Unveils India's Approach towards Regulating Artificial Intelligence." *Chambers and Partners*, 17 Nov. 2025, https://chambers.com/articles/meity-unveils-india-s-approach-towards-regulating-artificial-intelligence.

DLA Piper. "Data Protection Laws in India." *Data Protection Laws of the World*, DLA Piper, https://www.dlapiperdataprotection.com/?t=law&c=IN. Accessed 3 July 2026.

Fukuyama, Francis. *State-Building: Governance and World Order in the 21st Century*. Cornell UP, 2004.

Grindle, Merilee S. "Good Enough Governance: Poverty Reduction and Reform in Developing Countries." *Governance*, vol. 17, no. 4, 2004, pp. 525–48.

IAPP. "With Rules Finalized, India's DPDPA Takes Force." *IAPP*, 14 Nov. 2025, https://iapp.org/news/a/with-rules-finalized-india-s-dpdpa-takes-force.

Insights on India. "India AI Governance Guidelines 2025: Balancing Innovation and Trust." *Insights on India*, 8 Nov. 2025, https://www.insightsonindia.com/2025/11/08/india-ai-governance-guidelines/.

Khaitan & Co. "ERGO — India AI Governance Guidelines." *Khaitan & Co.*, 11 Nov. 2025, https://www.khaitanco.com/sites/default/files/2025-11/ERGO%20%20%20%20India%20AI%20Governance%20Guidelines%20-%2011%20November%202025.pdf.

Lexology. "India's Digital Personal Data Protection Regime Takes Effect." *Lexology*, 24 Nov. 2025, https://www.lexology.com/library/detail.aspx?g=2073ac40-628f-4112-81f3-fffdfd4b8858.

Mind of Cyber. "Cybersecurity of India in the Era of 2025: Strengths, Weaknesses, and the Road Ahead." *Mind of Cyber*, 6 Oct. 2025, https://www.mindofcyber.com/2025/10/06/india/.

Ministry of Electronics and Information Technology. *India AI Governance Guidelines*. Government of India, 5 Nov. 2025, https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.

Mondaq. "India's AI Governance Guidelines." *Mondaq*, 18 Feb. 2026, https://www.mondaq.com/india/new-technology/1746072/indias-ai-governance-guidelines.

National e-Governance Division. "AI for All: India's Blueprint for a Smarter Future." *National e-Governance Division*, 16 Sept. 2025, https://negd.gov.in/blog/ai-for-all-indias-blueprint-for-a-smarter-future/.

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

Press Information Bureau. "India AI Governance Guidelines." Government of India, 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228315.

Press Information Bureau. "Transforming India with AI." Government of India, 8 Oct. 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2209737.

Press Information Bureau. "Government of India Taking Measures to Protect Critical Infrastructure and Private Data against Cyber Attacks." Government of India, 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341.

Press Information Bureau. "Government Notifies DPDP Rules, 2025." Government of India, 14 Nov. 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014.

Press Information Bureau. *CERT-In: India's Frontline Defender against Cyber Threats*. Government of India, Jan. 2026, https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/jan/doc2026123764501.pdf.

RSM India. "India's Cybersecurity Policy Frameworks: Key Strategies and Initiatives." *RSM India*, 8 July 2025, https://www.rsm.global/india/insights/consulting-insights/cybersecurity-policy-frameworks.

Sai Krishna & Associates. "Decoding the India AI Governance Guidelines." *Sai Krishna & Associates*, 12 Nov. 2025, https://www.saikrishnaassociates.com/decoding-the-india-ai-governance-guidelines/.

Vision IAS. "CERT-In Handled around 30 Lakh Cyber Incidents in 2025." *Vision IAS*, 27 Jan. 2026, https://visionias.in/current-affairs/news-today/2026-01-27/security/cert-in-handled-around-30-lakh-cyber-incidents-in-2025.