LIRNEasia
Pro-poor. Pro-market.

Data Governance Framework: India

Data for Development — South and Southeast Asia

Pranesh Prakash

December 1, 2024

Table of contents

About this report

About LIRNEasia

LIRNEasia is a pro-poor, pro-market regional policy think tank. Our mission is *Catalysing policy change and solutions through research to improve the lives of people in the Asia and Pacific using knowledge, information and technology.*

Address: 15 2/1, Balcombe Place, Colombo 8, Sri Lanka.
Telephone: +94 11 267 1160
Email: info@lirneasia.net
Website: https://lirneasia.net/
Twitter: https://x.com/LIRNEasia
Facebook: https://www.facebook.com/lirneasia/
YouTube: https://www.youtube.com/@LIRNEasia-
LinkedIn: https://lk.linkedin.com/company/lirneasia
Instagram: https://www.instagram.com/lirneasia/

Funding

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada. The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

1 Introduction

This report on data governance in **India** is part of the 'Harnessing Data for Democratic Development in South and Southeast Asia' (D4DAsia) project, which aims, *inter alia*, to create and mobilise new knowledge about tensions, gaps and the evolution of the data governance ecosystem taking into account formal and informal policies and practices.

In today's digital age, data governance ecosystems play a crucial role in shaping our societies. These ecosystems, comprising policies, laws, practices, behaviours, and technologies, aim to govern data in ways that protect rights, foster innovation, enhance transparency, and ultimately promote democratic and inclusive governance. An ideal data governance system would protect rights, enable innovation, improve transparency, and help in bringing about democratic, inclusive governance. However, the landscape of data governance is complex and often fraught with challenges, particularly in South and Southeast Asia.

Through the rest of the report, unless the context indicates otherwise, the term 'policies' is used as shorthand for policies, statutes, regulations, rules, administrative orders and even practices and technologies that are used to implement all of those as part of data governance ecosystems.

Data is increasingly being recognised as an enabler for development. It is an essential requirement for policymaking and monitoring of development goals and targets. When effectively managed, data can be used as an asset to support significant development actions such as poverty reduction, food security, mitigating impact of climate change, and disaster management. If mismanaged, it can exacerbate inequalities and undermine the development potential of the same actions.

The D4DAsia project has produced nine reports so far: seven detailed individual country reports that deal with the issues of data governance in the following countries; India, Indonesia, Nepal, Pakistan, Philippines, Sri Lanka and Thailand; a detailed look at data protection in South Korea; and a synthesis report that summarises the findings from the various countries while drawing out the contrasts amongst them, along with detailed findings for the research questions we had posed. The questions are:

1. What is common, and what is nationally specific, in the emerging data governance architectures in South and Southeast Asia? What are the explanations?
2. What are the implications of the emergent nature of the governance architecture? Because there is no overall design that envisions how the parts fit together, it is likely that there will be friction points and even contradictions. How are these being worked out?
3. The emerging governance architecture involves trade-offs among objectives such as greater accountability of powerholders, economic growth, including the creation of employment and wealth, resilience of systems, etc. How have different societies: (a) explicitly recognised the trade-offs or not; and (b) handled them?
4. Are there legislative or policy innovations with potential for replication? What are the modalities of sharing experiences? Are developing countries learning from each other, or are they learning from the developed countries?
5. How were the laws and bills developed? What expertise was brought to bear? How open were the procedures? How receptive were drafters to suggestions and criticisms?
6. How were capacity challenges addressed: by simplifying the laws or by tolerating incomplete implementation?

1.1 Structure of the report

1.1.1 Governance background

This report starts by providing contextual information about the constitution and governance framework in **India**, including how lawmaking powers are distributed and delegated, the powers of the judiciary to overturn laws or to enforce policies, and the legal and regulatory background in the country.

1.1.2 Increasing openness/access

The report then discusses policies that increase openness or access. By this we mean policies that allow greater access by citizens, consumers, and corporations to data, or facilitate interoperability or cross-border data transfer. Specifically, we do not include increased governmental access to citizens' private data or non-public corporate data.

This section discusses open data policies, the question of how much governmental data is made available proactively and how much is reactive as well as the quality of data being disseminated. The report also assesses government policies favouring or requiring free and open source software (FOSS) or open standards, noting any specific standards that are mandated.

1.1.3 Decreasing openness/access

The report then moves on to discuss the opposite, i.e. laws, policies and practices that decrease openness or access. By this we mean decreasing access of citizens, consumers, and corporations to data. To be clear, this is not a negative value judgement, since upholding important individual and collective rights, such as privacy and public security, necessitate reducing citizens' access to data.

This theme explores issues of security such as whether there are any data retention or localisation requirements, restrictions on the right to access information (such as national security, privacy etc.) and exceptions to data security requirements for law enforcement. We further discuss the privacy and copyright framework in brief and specifically try to answer whether there are any exceptions for search engines as well as for research and artificial intelligence (AI).

The issue of data governance and the policies surrounding its implementation is a critical one for governments, citizens and businesses across the world. As mentioned earlier, we use the term data governance to refer to 'diverse arrangements, including technical, policy, regulatory or institutional provisions, that affect data and their creation, collection, storage, use, protection, access, sharing and deletion across policy domains and organisational and national borders.'[1]

[1] OECD, *Going Digital Guide to Data Governance Policy Making*.

2 Overview

2.1 Legal framework

Before getting into questions around data governance (including what precisely that term is used to refer to in this report), it might be useful to first give a brief description of the Indian legal system. India is a constitutional republic and a union of states. It mostly follows the common law system, but it also recognizes customary law, and, in matters of personal/civil laws, accepts religious laws for some religions, while having codified laws for others.

2.1.1 Constitution of India

The Constitution of India provides the basic framework for governance; division of powers between the union and states, separation of powers between the parliament, the executive and the judiciary; and provisions for fundamental rights which cannot be abrogated or rescinded by the government, though they may be reasonably restricted for specific purposes as provided for in the Constitution itself.

2.1.2 Union and state legislatures

The power to legislate is provided to both the union and states, via the parliament and state legislative assemblies, respectively. The Constitution contains three lists which enumerate subject matters that shall be the exclusive prerogative of the union, the states, and a list on which either or both can legislate. Unlike in countries like the United States, unenumerated subjects are reserved for the union rather than the states. Statutes that have been introduced but not yet passed are called "bills", which become "acts" once they are passed.

2.1.3 Executive lawmaking

The government has power to pass subordinate legislation when provided for in each law, but those have to be laid before the Parliament in case the statute provides for the same. This, in reality, is a mere formality, since almost no subordinate legislation has ever been scrutinized by Parliament even though it not only has the power but also the obligation (given separation of powers) to do so.

The union and state governments' executive powers are coextensive with the powers of the union and state legislatures. So, the union government cannot take action on subject matters that fall within the realm of state governments under the Constitution.

2.1.4 Judicial review

The higher judiciary has the power of judicial review, meaning that it can strike down laws passed by the legislative branch, apart from adjudicating on the legality of executive action.[2] A High Court or the Supreme Court can strike down a law or executive act in the following circumstances: If the law violates any fundamental right guaranteed under Part III of the Constitution (such as right to equality, freedom of speech and expression, right to life and personal liberty, etc.); if the law is beyond the legislative competence of the legislature that enacted it, in accordance with the distribution of powers under the Constitution; if the law or

[2] Sorabjee, "Introduction to Judicial Review in India," 126.

constitutional amendment violates the 'basic structure' of the Constitution — that damage or destroy the basic features like secularism, separation of power, parliamentary democracy, etc.; or if the law is passed without following the proper legislative procedure as laid down in the Constitution.

2.2 Outline of the report

The report is divided into two broad parts: a mapping of the laws and policies that impact data governance and then a deeper dive into the data protection landscape in India as well as 'India Stack', a set of API-based digital infrastructure promoted by the Indian government, which are now being re-branded as "digital public infrastructure" and "digital public goods".

The mapping of laws and policies, in turn, is divided into two parts: laws and policies that increase openness — covering open standards, free/libre/open source software, open data, right to information, and so on — and those that decrease openness — privacy laws, national security-linked laws, copyright laws, etc.

3 Laws and policies impacting data governance

This section seeks to map laws and policies in India that relate to data governance. Given that there are hundreds of laws that have some kind of impact or another on data, the attempt here is not to be exhaustive, but to cover all the major laws and policies that relate to data governance. As mentioned previously, in this section, we'll be discussing both policies that increase openness / access and those that decrease openness / access.

3.1 Increasing openness and access

By "increasing openness and access", we mean something that increases or safeguards citizens' or companies' access or liberties in relation to public data or reduces access by the government to citizens' or companies' data. This consists of both technological openness in the form of open standards and free/libre/open source software, and also various forms of open data and open content.

3.1.1 Open standards / free, libre, open source software

"When it comes to economic, social and cultural rights (ESCRs) in an information society, free software and open standards are both particularly significant."[3] In terms of the International Covenant on Economic, Social, and Cultural Rights (ICESCR), by promoting open access to software and information, free and open source software (FOSS) and open standards further Article 13's call for equal access to education. FOSS's royalty-free nature also fulfills Article 15(1)(b)'s aim of cultural participation for all by enabling access regardless of financial means. Wide adoption of FOSS and open standards by governments enables the right to work under Article 6, as workers can gain transferable digital skills and apply them using freely available tools. Overall, FOSS and open standards are critical for realizing the ICESCR's vision of equitable access to education, technology, culture, and work opportunities for all.[4]

Open standards and interoperability

Interoperability in data governance is essential for ensuring that different systems and organizations, including governments, can seamlessly exchange and use data. By reducing silos and fostering collaboration, interoperability enables data to be used across different software and systems, improving efficiency and innovation and adaptability.

While there is no universal definition of what an open standard is, in this paper we're using the term "open standard" to refer to technical standards that are made publicly available and can be used by anyone without having to pay royalties. In other words, open standards are free to use and implement, and are not controlled by a single company.

Government

1. National Policy on the Use of Open Standards in e-Governance, 2010
2. Interoperability Framework for e-Governance, 2015
3. Guidelines for Indian Government Websites, 2009 / 2018 / 2023

---

[3] Abraham and Marda, *Free and Open Source Software (FOSS) and Open Standards.*

[4] Abraham and Marda.

4. Rights of Persons with Disabilities Act, 2016 read with Rule 15, Rights of Persons with Disabilities Rules, 2017

The Bureau of Indian Standards (BIS) is the national standards body and represents India at the International Standards Organization. Apart from the BIS, for government standards, the STQC (Standardisation Testing and Quality Certification) Directorate under the Ministry of Electronics and Information Technology (MeitY) plays a crucial role. STQC is responsible for developing and promoting quality assurance standards for electronic products and IT systems.

In 2010, India adopted a national policy[5] on the use of open standards in e-governance.[6] This policy required that royalty-free standards be used by the government for all purposes, while allowing for proprietary standards to be used if suitable open standards were unavailable. In pursuance of this policy, various e-Gov standards were also notified. However, these policies have not been very successful in terms of implementation. Further, being mere policies (rather than regulations or statutory law), they are not justiciable — meaning they cannot be enforced via a court proceeding.

Additionally, the central government has formulated 'Guidelines for Indian Government Websites' (GIGW),[7] with the aim to "ensure quality and accessibility of government guidelines, by offering guidance on desirable practices covering the entire lifecycle of websites, web portals and web applications, right from conceptualisation and design to their development, maintenance and management."[8] The first version of the GIGW was released in 2009, the second in 2018, and the third, which is the most recent, in 2023. Through the GIGW, the government has adopted the Worldwide Web Consortium's Web Content Accessibility Guidelines (WCAG) — a globally recognized standard for web accessibility — for governmental websites and apps, thus seeking to ensure conformity with Level AA of WCAG 2.1. However, an analysis by CIS in 2012 showed that most governmental websites were not fully accessible even three years after the adoption of the GIGW,[9] as did a follow-up report in 2016. A more recent paper[10] also comes to similar conclusions, noting "e-government websites give low priority to [compliance with accessibility standards] during website design and development." Under the GIGW, government departments are required to submit their website content for accessibility checks to the Standardisation Testing and Quality Certification (STQC) directorate. Separately, the National Informatics Centre has developed a tool called SugamyaWeb[11] which can be used by accredited government website managers to check for WCAG 2.0 and WCAG 2.1 compliance.

The Indian government has also been pushing the idea of "Digital Public Infrastructure". These are often said to be interoperable, implementing open standards, and built using open source software. For instance, in the 2023-24 Union budget speech, the Finance Minister[12] said that "the Digital Public infrastructure for agriculture will be built as an open source, open standard and interoperable public good."

---

5 Hariharan, "Open Standards Policy in India."

6 Policy on Open Standards for e-Governance.

7 National Informatics Centre, "Guidelines for Indian Government Websites and Apps 3.0."

8 National Informatics Centre, 7.

9 Narasimhan et al., *Accessibility of Government Websites in India: A Report*.

10 Paul and Das, "Accessibility and Usability Analysis of Indian e-Government Websites."

11 National Informatics Centre, "SugamyaWeb."

12 Press Information Bureau, "Summary of the Union Budget 2023-24."

Private sector

1. Companies (Filing of documents and forms in Extensible Business Reporting Language) Rules, 2011, and numerous notifications and circulars following this.

Some open standards have been mandated for use by the private sector as well. The Ministry of Corporate Affairs (MCA) has implemented the MCA21 project, which seeks to provide easy and secure online access to all registry related services provided by the MCA to corporate entities, professionals and citizens of India. The MCA21 project uses the XBRL (eXtensible Business Reporting Language) standard for filing financial statements by companies. XBRL is an open and global XML-based standard for exchanging business information in a digital format, enabling the automation of business information processing.

Apart from this, organizations like Indian Software Product Industry Roundtable (iSPIRT), which have been involved in the development of various technologies like Unified Payments Interface (UPI) and Digilocker, have pushed for open standards to be adopted as part of "India Stack,"[13] which, in turn, would enable the private sector to adopt open standards to interact with India Stack. Further, the Open Network for Digital Commerce (ONDC) has been launched by the government as a private company aimed at "promoting open networks for all aspects of exchange of goods and services over digital or electronic networks", and as part of that seeks to "standardize operations like cataloguing, inventory management, order management and order fulfilment."[14] The ONDC itself is based on an open standard called Beckn Protocol.

Free / libre / open source software

1. Kerala Information Technology Policy Document, 2001
2. Kerala Information Technology Policy, 2007
3. Assam Information Technology Policy, 2009
4. National Policy on Information Technology, 2012
5. Policy on Adoption of Open Source Software for Government of India, 2014
6. Policy on Collaborative Application Development by Opening the Source Code of Applications, 2015
7. Draft Kerala Information Technology Policy, 2023

There have been policies both at the state level and the national level with regard to adoption of Free/Libre/Open Source Software (FOSS).

At the national level, the National Informatics Centre (NIC) started propagating FOSS as early as 2004, by establishing a stand-alone site to share the Indian government's experience with FOSS.[15] In 2005, the Centre for Development of Advanced Computing (C-DAC) was founded as a government body that works to promote India's FOSS capacity. That same year, the Indian government established the National Resource Centre for Free & Open Source Software (NRCFOSS). Its major goals include developing human resources around FOSS, developing FOSS — including localization of software, and the development of the BOSS Linux operating system designed for the use of Indian government agencies — policy formulation, and encouraging FOSS entrepreneurs. It also seeks to "provide design, development and support services to the FOSS community in the country."[16]

---

13 Matthan and Ramann, "India's Approach to Data Governance - Data Governance, Asian Alternatives."
14 "ONDC Project."
15 Loney, "India Shares Open-Source Experience."
16 Ministry of Electronics and Information Technology, "Major FOSS Initiatives."

BOSS GNU/Linux, developed by C-DAC and NRCFOSS, is a Debian-based operating system aimed at promoting Free/Open Source Software in India. It features a GNOME desktop with wide Indian language support and government-relevant packages. BOSS is localized for most Indian languages and is used by various government agencies and defence establishments.[17] EduBOSS is a companion distribution focused on school education.[18]

The National Policy on Information Technology, 2012 had as one of its objectives, "adopt[ing] open standards and promot[ing] open source and open technologies".[19] This was followed in 2014 by the Policy on Adoption of Open Source Software for Government of India,[20] which provided a policy framework for rapid and effective adoption of open source software in all e-Governance systems implemented by various government organizations. The policy stated that all software deployed by the government must be open source — allowing the rights to study, modify, and redistribute copies of the original or modified software — unless there's a documented justification for proprietary software to be used. While the policy states that it is mandatory, it is legally unenforceable in a court since it is a policy and not a law.

In 2015, it followed this up by adopting a "Policy on Collaborative Application Development by Opening the Source Code of Applications."[21] This policy seeks to promote "reuse, standardization, innovation, quality improvement and cost savings through collaboration and avoidance of duplication" as well as to "improve the overall quality and security through increased transparency and mass peer review". It does so by mandating that any new software developed in-house or procured through a contract have its source code be made publicly available, along with installation scripts, documentation, database schemas, etc. The policy, however, does not note what licence the source code should be made available under, nor does it lay out what licence contributions from third parties will be made under. A collaborative code hosting platform called OpenForge was set up under this policy. So far, this policy has not been very effective.

At the state level, Kerala has been an exemplar in the adoption of FOSS, acknowledging its role as early as 2001 in the state IT Policy. By 2011, the International Centre for Free and Open Source Software (ICFOSS) was fully functional: an autonomous organization under the Kerala government, it has a broad mandate to promote FOSS. The integration of FOSS into the Kerala education system has been studied extensively.[22]

The 2009 Assam IT Policy included a section of FOSS that sought to promote the use of FOSS in all departments and state agencies; promote training in the use of FOSS, including in schools and colleges; preferential tendering for FOSS; source code of government-developed or -customized software to be made publicly available; use of open standards such as open document format (ODF); and use of hardware that supports FOSS operating systems.[23] None of these policies are enforceable.

Outside of government tenders, there are no policies or laws that require the private sector to use FOSS. However, there are private organizations like the Free Software Movement of India, Swecha, IT for Change, the Centre for Internet and Society, FOSSCOMM, and most recently FOSS United that have sought to push the adoption of FOSS not only in e-governance, but also

---

17 Centre for Development of Advanced Computing, "C-DAC Free/Open Source Software."
18 Centre for Development of Advanced Computing, "C-DAC Free/Open Source Software."
19 National Policy on Information Technology.
20 Policy on Adoption of Open Source Software for Government of India.
21 Policy on Collaborative Application Development by Opening the Source Code of Applications.
22 Krishnaswamy and Marinova, "Free and Open Source Software (FOSS) in Education."
23 Information Technology Policy of Assam.

in the education system, and seek to encourage the use of FOSS by all, including the private sector.

3.1.2 Open data / content / data sharing

This section covers laws relating to the public access to publicly-funded content of various kinds and state-held data. This may be in the form of statistical data collected by the state, regulations related to archiving, the right to information which is crucial for transparency of governmental functioning, or proactive publication of data on open data portals. In this context, "open data" refers to data or content made available in a machine-readable format (e.g., no scanned image-only PDFs), and under a permissive copyright licence that allows for permission-less use by all, regardless of purpose.

Statistical data

1. Census Act, 1948
2. Collection of Statistics Act, 1953
3. Collection of Statistics Act, 2008
4. Registration of Births and Deaths Act, 1969
5. Guidelines for Statistical Data Dissemination, 2019

For a well-functioning polity, the collection and open dissemination of statistics is imperative. National- and state-level statistics is a public good provided by the government. In India, the Census Act, 1948 is the oldest law that governs the collection of statistics in independent India. This law governs the conduct of the decennial census that's been conducted in India since 1872 (the latest census was to be conducted in 2021 but has still not been conducted); it requires the government to collect and publish demographic, social, and economic data on the population of India. One trade-off it manages relates to privacy. While Sections 7 and 8 of the Act impose a duty upon citizens to provide truthful and accurate responses to census questions, Section 15 makes those responses confidential, preventing them from being used for any purpose other than aggregation of data — the responses cannot even be used in civil or criminal proceedings.

During the very first term of parliament, after India's independence, the Collection of Statistics Act, 1953 (CoS Act 1953) was passed, as statistics was seen as very important for the socialistic planning economy that India was pursuing. The CoS Act 1953 was limited to statistics on industry, labour, trade and commerce. It made it mandatory to share information with the government when required to do so. While it prohibited publication of information with regard to individual entities without their consent, it did allow for use of such information for criminal prosecutions. Apart from the CoS Act 1953, various sector-specific legislations governed the collection of statistics. With increased privatization and liberalization, the Rangarajan Commission noted in 2001, a dent was created in India's statistical system.[24] They recommended a new law with an expanded focus. This led to the Collection of Statistics Act, 2008, being passed. The new Act allows for statistics to be collected on economic, demographic, social, scientific and environmental issues, not just from industrial and commercial establishments but also from households and government agencies.[25] As with the 1953 Act, the 2008 Act also requires that informants provide information that is true to the best of their knowledge or belief, on pain of penalty. The 2008 Act has specific provisions on security and privacy of the collected information,[26] but it doesn't *explicitly* disbar information relating to individuals from

[24] Central Statistics Office, *Handbook on the Collection of Statistics Act, 2008.*
[25] The Collection of Statistics Act, § 3 and 5.
[26] The Collection of Statistics Act, s.9.

being disclosed in a civil or criminal proceeding, and only does so *implicitly*. Still, the Act makes it clear that any publication of the data should prevent any specific informant from being identified, except with the consent of the informant.

In 1969 the Registration of Births and Deaths Act was enacted, which mandated that births and deaths be registered with the local Registrar within 21 days of the occurrence. The data collection and management happens through state-level agencies, while the central government coordinates and sets parameters for what data needs to be collected. Through this, the Act aims to create a uniform system for registering vital events and maintaining accurate vital statistics, and also providing for the legal recognition of births and deaths, which is important for establishing identity, inheritance rights, and access to various services and benefits. While historically, the civil registration system has functioned rather poorly in India by not registering many births and especially deaths, this has changed in recent years. As the Vital Statistics Division[27] notes, "The registration level of births for the country has gone up to 92.7% in 2019 from 82.4% in 2011," and "registration level of deaths during 2019 has increased to 92.0% from 66.4% in 2011."

The central government currently conducts a number of surveys, including the National Family Health Survey (NFHS), National Sample Survey (NSS), Socio-Economic and Caste Census (SECC), Periodic Labour Force Survey (PLFS), Annual Survey of Industries (ASI), Economic Census, District Level Household Survey (DLHS), and the Comprehensive National Nutrition Survey (CNNS). State-level surveys, including on households, agriculture, and employment, are conducted by some states. The data from these surveys are available in open formats both at their specific websites, as well as from the data.gov.in portal.

In 2019, the Ministry of Statistics and Programme Implementation published its Guidelines on Data Dissemination, in keeping with the NDSAP 2012. Accordingly, it categorized data into four categories: open access data, restricted access data (free of cost), restricted access data (priced), and non-shareable data. The non-shareable data includes exception for areas designated sensitive by the military, and data sets containing identification particulars of individual informants or establishments, or which may lead to their identities being uncovered. Thus national security and privacy

Whenever census or survey data is published, the perennial concern is the trade-off between data accuracy and utility versus privacy. Indian laws seek to explicitly negotiate that trade-off by ensuring that individual-level privacy is maintained at all times.

Right to information

Proactive disclosure

1. Section 4, Right to Information Act, 2005
2. Consumer Protection Act, 2019

In 2005, learning from the problems with previous versions of transparency laws in India, the central government adopted the Right to Information Act.[28] Among the provisions of this law is a mandate to maintain and proactively make available various governmental information and policies.[29] Proactive disclosure is a key feature of the Right to Information Act, which aims to promote transparency and accountability in the functioning of public authorities. Section 4 of

[27] "Civil Registration System."
[28] Right to Information Act.
[29] Section 4, Right to Information Act.

the Act requires every public authority to publish and disseminate various kinds of information, such as its norms, rules, regulations, policies, decisions, budget, subsidies, beneficiaries, etc..[30] The purpose of proactive disclosure is to reduce the need for citizens to file RTI requests and to make the information easily accessible to the public.

Section 4(b) of the Act specifies 17 categories of information that every public authority must proactively disclose on its website and update regularly.[31] Some of these categories are: the particulars of the organization, functions and duties; the powers and duties of its officers and employees; the procedure followed in the decision making process; the monthly remuneration received by each of its officers and employees; the details of the budget allocated to each of its agencies; the manner of execution of subsidy programmes; the particulars of recipients of concessions, permits or authorizations granted by it; and the details of the information available to or held by it, reduced in an electronic form.[32]

The Supreme Court of India has issued guidelines to the Central and State Information Commissions to ensure the proper implementation of Section 4 of the RTI Act.[33] The guidelines include: monitoring the compliance of public authorities with Section 4; issuing directions to public authorities to make proactive disclosures in accordance with Section 4; conducting periodic audits of the websites of public authorities; imposing penalties on the officers responsible for non-compliance with Section 4; and creating awareness among the public about the benefits of proactive disclosure. The guidelines also suggest that public authorities should adopt a digital proactive disclosure policy, which would enable the automation of proactive disclosure and the creation of a centralized, machine-readable database of data like contracting data.

The Consumer Protection Act, 2019 includes a "right to be informed" about the quality, quantity, potency, purity, standard, and price of goods or services. However, this right is not a directly enforceable right, and has been included to give the consumer protection authorities the discretionary power to take action to protect consumer rights.

Reactive disclosure

1. Right to Information Act, 2005

While the RTI Act provides for proactive disclosure, the bulk of the Act deals with reactive access to information held by the government. The RTI Act was passed after years of grassroots campaigning by organizations like the Mazdoor Kisan Shakti Sangathan (Association for the Empowerment of Labourers and Farmers) and the National Campaign for People's Right to Information, and despite stiff bureaucratic opposition. The law allows citizens to write to designated public information officers (PIOs) seeking any kind of information that is within the possession of the PIO. The government of India even has an online portal (https://rtionline.gov.in/) using which RTI queries may be submitted online. The PIO is obligated to mandatorily provide a response within 30 days of the query. If the PIO does not respond within 30 days, or otherwise obstructs the request, or provides false, misleading or incomplete information, then the PIO — not the public authority — is personally liable to pay a penalty. These strict provisions have led to India being seen as a global leader in the right to information. A global RTI ranking project notes, "India has long been recognised as an advanced country when it comes to the right to information, but its dropping ranking in the RTI Rating shows that global

[30] Section 4(a), Right to Information Act.
[31] Section 4(b), Right to Information Act.
[32] Section 4(b), Right to Information Act.
[33] *Kishan Chand Jain v. Union of India.*

standards on the right to information have advanced considerably since India's law was first passed in 2005. It remains one of the top ranked countries in the world but there are several problems with India's access regime."[34]

A 15-year review by Transparency International India[35] noted that the implementation of the Right to Information (RTI) Act faces significant challenges across its key stakeholders: State Information Commissions, Public Information Officers (PIOs), and Information Seekers. State Information Commissions suffer from a lack of political will, inadequate infrastructure, and high levels of vacancy and backlog, which hinder their effectiveness. Public Information Officers struggle with poor record management, insufficient training, and heavy workloads, all compounded by a lack of motivation and incentives. Information Seekers, especially marginalized groups, face low awareness, inconsistent rules, uncooperative PIOs, and even intimidation, leading to poor quality responses and a lack of confidence in the system. These issues collectively undermine the potential of the RTI Act to promote transparency and accountability.

Amongst the tensions that the RTI Act seeks to resolve are those between transparency and privacy, national security, intellectual property rights, foreign relations, and excessive scrutiny of executive decision-making, etc. There are exceptions listed in Section 8 and 24 — the latter of which exempts specific intelligence agencies from the operation of the RTI Act. The government has previously held workshops on the conflict between transparency and privacy (2012). However, in 2023, Parliament passed the Digital Personal Data Protection Act, which did away with the balancing test provided in Section 8(1)(j),[36] without any public consultation. This will be examined later in this paper.

Open government data

Open government data (OGD) refers to government data that is freely available for anyone to access, use, and share. When governments implement open data policies, they enhance transparency, foster innovation, and empower citizens and businesses by providing access to valuable information that can be used for research, policy-making, and creating new services and products. The following policies affect open government data (OGD) in India:

1. National Data Sharing and Accessibility Policy, 2012
2. NDSAP Implementation Guidelines, 2015
3. Sikkim Open Data Acquisition and Accessibility Policy, 2014
4. Odisha State Data Policy, 2015
5. Telangana Open Data Policy, 2016
6. Punjab State Data Policy, 2020
7. Data Sharing And Accessibility Policy For Chandigarh Smart City Limited, 2020
8. Karnataka Open Data Policy, 2021
9. Tamil Nadu Data Policy, 2022

In 2010, the Centre for Internet and Society published the earliest report on open data in India, cataloguing existing practices, analysing laws including on privacy and copyright, and providing recommendations on laws, policies, and practices required for effective promotion and use of open data.[37] In 2011, when the Open Government Partnership (OGP) was being formed, India

---

34 Centre for Law and Democracy and Access Info Europe, *Global Right to Information Rating*.

35 Jha et al., *State Transparency Report*.

36 Right to Information Act.

37 Wright et al., *Open Government Data Study: India*.

initially expressed an intent to join, but eventually did not do so.[38] Yet, in 2011, the government announced that it would be launching an open data portal, and in 2012 followed up on that commitment by publishing a policy to govern publication of central government data.

The National Data Sharing and Accessibility Policy (NDSAP) was introduced by the Indian government in 2012. The policy encourages the sharing of non-sensitive data generated using public funds by various arms of the Government of India and State Governments. The stated aim was to increase accessibility and easier sharing of non-sensitive data amongst registered users for scientific, economic, and social developmental purposes.[39]

The policy mandates the classification of all governmental data and making available non-classified data as open data. Soon after, the government launched data.gov.in[40] as a unified portal to function as a single-point access to datasets, documents, services, tools, and applications published by ministries, departments, and organizations of the Government of India. This platform is part of the government's Open Government Data initiative, aiming to promote transparency, increase citizen engagement, and improve decision-making. The data.gov.in portal has had a mixed record. A review in 2015 noted that while it has published over 18,000 resources and received millions of views and downloads, critical datasets were often unavailable, outdated, duplicated, or lacked proper metadata.[41] The government's open data policies have not been implemented consistently across agencies, resulting in inconsistent data sharing: while some datasets are well-curated, others are not. While there has not been a good survey of the portal, recent impressions are that the situation is improving.

To implement NDSAP, the Indian government introduced the NDSAP Implementation Guidelines in 2015.[42] These guidelines provide a framework for data sharing and accessibility, promoting interoperability of both scientific and technical data.

In 2017, the government published the "Government Open Data Licence – India" licence under which all the material released under the NDSAP are licensed.[43] This licence explicitly excludes personal information from the scope of the licence, along with information of the categories listed under Section 8 of the RTI Act, showing that trade-offs were considered, and a cohesive approach was followed, with references to existing laws.

Several states and even some cities in India have passed their own open data policies: Sikkim Open Data Acquisition and Accessibility Policy, 2014; Odisha State Data Policy, 2015; Telangana Open Data Policy, 2016; Punjab State Data Policy, 2020; Data Sharing And Accessibility Policy For Chandigarh Smart City Limited, 2020; Karnataka Open Data Policy, 2021; and the Tamil Nadu Data Policy, 2022.[44] There has been no systematic study of the effectiveness of these policies.

Open access to scholarly literature

1. University Grants Commission Mandate, 2009
2. CSIR Open Access Mandate, 2011
3. Indian Council of Agricultural Research Open Access Mandate, 2013

---

38 Dey and Roy, "India in Open Government and Open Government in India."
39 National Data Sharing and Accessibility Policy.
40 Ministry of Electronics and Information Technology, "Open Government Data (OGD) Platform India."
41 Agarwal, "India Must Do More to See Impact of Open Data."
42 OGD Division, NIC, *Implementation Guidelines for NDSAP*.
43 Government Open Data Licence.
44 Panjiar and Prateek Waghre, "A Comparison of State-Level Data Policies."

4. Delhi Declaration of Open Access, 2018
5. Science, Technology, and Innovation Policy 2020

There has been a movement in India to increase open access to scholarly literature since at least 2004.[45] In 2011, a group of 39 government labs (CSIR) adopted an open access mandate.[46]

Academic institutions have developed digital archives, known as institutional repositories, to collect and preserve their scholarly works electronically. These repositories make research outputs freely available and searchable by the general public. They typically contain a variety of academic materials, including research articles, literature reviews, theses, dissertations, reports, and both pre- and post-print versions of papers.

As of spring 2020, the Open Directory of Open Access Repositories (OpenDOAR), based in the United Kingdom, had indexed 92 such repositories in India. In addition to these institution-specific archives, India has also established several national-level repositories to advance open access initiatives. A notable example is Shodhganga, India's central repository for doctoral theses. By April 2020, Shodhganga, managed by the Information and Library Network (INFLIBNET), had amassed a collection of nearly 270,000 full-text Ph.D. theses from over 430 universities across the country.

Another massive undertaking by the government of India, in collaboration with the Indian Institute of Technology at Kharagpur, is the National Digital Library of India. This digital library collates, catalogues, and provides access to over 107 million items,[47] and is built using free/open source software and open standards, including open metadata standards.

Open geospatial data

1. National Map Policy, 2005
2. 2021 Guidelines under the National Map Policy, 2005

Geospatial data refers to the information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth. Geospatial data can be used for various purposes, such as mapping, navigation, disaster management, urban planning, environmental monitoring, and national security. However, the access and use of geospatial data in India has been historically restricted by various legal and policy barriers, which have hampered the development and innovation of the geospatial sector in the country. India has a rich and diverse heritage of geospatial knowledge, dating back to ancient times, when Indian scholars and cartographers produced accurate and detailed maps of the Indian subcontinent and beyond. However, India's colonial legacy and post-independence security concerns have led to a culture of secrecy and control over geospatial data, which has prevented its optimal utilization and dissemination for public good.

One of the main barriers to open geospatial data in India was the National Map Policy 2005.[48] The NMP 2005 defined the scope, distribution and liberalized access of digital Survey of India (SOI) topographic maps to user groups without jeopardizing national security. However, the NMP 2005 also imposed several limitations and conditions on the access and use of geospatial data, such as:

---

45 Rajashekar, "Open-Access Initiatives in India."
46 Open Access Mandate.
47 *Wikipedia*, "National Digital Library of India."
48 "Open Geospatial Data from Government of India - OpenStreetMap Wiki."

- The prohibition of the export of all maps and digital data in 1:250,000 and larger scales through any means.
- The licensing of digital maps to only Indian individuals, organizations, firms or companies, and the prohibition of unauthorized copying and distribution of SOI digital data.
- The requirement of a one-time clearance from the Ministry of Defence (MoD) for accessing the Open Series Maps (OSMs), and the registration of all transactions relating to digital maps in an online Map Transaction Registry (MTR) maintained by the SOI.
- The requirement of certification from the SOI for publishing maps on hard copy and web with or without GIS database, especially if the international boundary was depicted on the map.

The NMP 2005 was criticized by many stakeholders, such as academics, researchers, civil society groups, and private sector entities, for being too restrictive, outdated, and inconsistent with the global trends of open data and geospatial technology.

In response to the growing demand and need for open geospatial data in India, the Central Government announced the new Guidelines for acquiring and producing Geospatial Data and Geospatial Data Services, including Maps, under the NMP 2005 on February 15, 2021.[49] The guidelines aim to liberalize the geospatial sector in India by removing the existing restrictions and enabling greater access and use of geospatial data by various stakeholders, such as individuals, companies, organizations, and government agencies. In 2022, the NMP was replaced by a National Geospatial Policy.

The National Geospatial Policy emphasizes openness and open standards as critical components for fostering innovation and interoperability in the geospatial sector.[50] By promoting open standards, open data, and platforms, the policy aims to enhance data accessibility and ensure seamless integration across various geospatial applications. It encourages the adoption of best practice standards to enable interoperability and support the creation of integrated geospatial information systems. This approach aligns with global best practices, drawing inspiration from frameworks like the Integrated Geospatial Information Framework (IGIF) and the UN-GGIM. In terms of permissions for mapping activities in India, the policy has deregulated map-making processes to encourage domestic innovation and competitive practices within the global mapping ecosystem. This contrasts with the National Mapping Policy 2005, which had more stringent regulations. The new policy simplifies rules related to aircraft and drone usage for surveying, promoting a more open environment for private sector involvement. It also introduces a more collaborative approach, where private entities play a significant role in geospatial data creation and management, whereas previously the Survey of India had a more central role. This deregulation aims to reduce duplication, streamline data management, and enhance the overall effectiveness of geospatial infrastructure.[51]

Traditional Knowledge Digital Library

India's Traditional Knowledge Digital Library (TKDL) is an initiative launched by the Council of Scientific and Industrial Research (CSIR) in collaboration with the Ministry of Ayurveda, Yoga & Naturopathy, Unani, Siddha, and Homoeopathy (AYUSH). It aims to protect Indian traditional knowledge from being enclosed using patents and from "biopiracy" (the unauthorized commercial use of biological resources and associated traditional knowledge) by commercial interests.

---

[49] Prakash and Anwar, "Two Experts Decode New Mapping Policy Guidelines, Explain Why This Is a Giant Leap Forward for India."

[50] National Geospatial Policy, clause 3.6.

[51] National Geospatial Policy, clause 5.2.1.

Established in 2001, the TKDL was a response to a notable biopiracy incident involving an American university. In 1995, the US Patent and Trademark Office granted a patent for the use of turmeric in wound healing, despite it being well-documented traditional knowledge in India. The CSIR successfully challenged this patent, providing evidence from ancient texts that led to its revocation in 1997. This landmark case highlighted the need for a systematic approach to protect traditional knowledge from being misappropriated.

The TKDL addresses this challenge by translating and structuring ancient texts on Ayurveda, Siddha, Unani, Sowa Rigpa, and Yoga into five international languages—English, Japanese, French, German, and Spanish. Using a Traditional Knowledge Resource Classification (TKRC) system, the TKDL has transcribed over 4.54 lakh formulations and practices, making them accessible to patent examiners worldwide. This classification seeks to make prior art searches during the examination of patent applications easier, thereby preventing the grant of wrongful patents. The TKDL uses digital technologies to preserve, protect, and promote India's rich heritage of traditional knowledge while respecting the rights of indigenous and local communities.

3.1.3 Open APIs

1. Policy on Open APIs for Government of India, 2015

APIs (Application Programming Interfaces) are sets of protocols and tools that allow different software applications to communicate and interact with each other. When governments implement open APIs, they can facilitate seamless data sharing, improve transparency, enhance service delivery, and enable developers to create innovative solutions that integrate with government systems, ultimately making public services more efficient and accessible.

India passed a "Policy on Open APIs for Government of India" in 2015.[52] This policy emphasises interoperability: "Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. It is also required in order to facilitate the single window concept of electronic services delivery by Government organizations."[53] The policy sought to ensure that all Government organisations published APIs for all eGovernance applications and systems.[54] Interestingly, this policy explicitly seeks to build upon the NDSAP (2012), the National Policy on Open Standards for e-Governance (2014) and the National Cyber Security Policy, showing that the policymakers did not look upon this as an ad hoc policymaking exercise, and took a comprehensive view.

The 2019 National Policy on Software Products[55] proclaimed that "implementation of open APIs will be proactively promoted both for public and private sector to foster incremental innovation and to encourage interoperability in Indian software products ecosystem." Despite the policy having been promulgated, it was difficult to find out about the APIs of different departments even when they existed. To combat this, in 2020 the government created an open API platform known as "API Setu."[56] This website provides a directory of central and state government APIs, and also APIs of private companies in sectors like insurance.

---

52 Policy on Open Application Programming Interfaces (APIs) for Government of India.
53 Policy on Open Application Programming Interfaces (APIs) for Government of India, 1–2.
54 Policy on Open Application Programming Interfaces (APIs) for Government of India, 2.
55 National Policy on Software Products.
56 Ministry of Electronics and Information Technology, "API Setu."

3.2 Decreasing openness / access

There are multiple policies that are aimed at decreasing openness, access to data, the free flow of data across national boundaries, or make it mandatory to store data for governmental use, but which the public cannot access. These can be for reasons of collective rights / common good / national security, etc., for instance policies relating to cybersecurity. Or these can be for reasons of individual rights, such as policies aimed at safeguarding individual privacy or the rights of copyright holders.

3.2.1 Collective rights / common good / national security

Data localization

1. Official Secrets Act, 1923
2. RBI Notification on Storage of Payment Data
3. RBI Directions on Outsourcing of Financial Services by NBFCs, 2017
4. Companies (Accounts) Rules, 2014
5. CERT-In's Cyber Security Directions, 2022
6. Unified Access Licence by the Department of Telecommunications
7. Public Records Act, 1993
8. IRDAI (Maintenance of Insurance Records) Regulations, 2015
9. SEBI Framework for Adoption of Cloud Services by SEBI Regulated Entities
10. SEBI Advisory regarding SaaS-based Solutions
11. Digital Personal Data Protection Act, 2023
12. RBI Master Direction on KYC, 2016 (amended in 2021)
13. Consolidated FDI Policy, 2020

The Official Secrets Act, 1923 is an anti-espionage law that prohibits any person from obtaining, collecting, publishing or communicating any information that might affect the security or interests of the state. The Act gives wide powers to the government to declare any area, place, document or information as a prohibited or notified area, and to search, seize, arrest and prosecute any person who violates the Act. The Act also imposes penalties of imprisonment and fine for any offence under the Act. The Act restricts the free flow of data by creating a culture of secrecy and limiting the access and dissemination of information that might be of public interest or importance.

The RBI Notification on Storage of Payment Data requires all system providers to ensure that the entire data relating to payment systems operated by them is stored in a system only in India. The data includes end-to-end transaction details and information pertaining to payment or settlement transactions that are gathered, transmitted or processed as part of a payment message or instruction. The system providers have to report compliance to the RBI and submit the system audit report conducted by CERT-In empanelled auditors. The notification aims to ensure better monitoring and supervision of payment systems and data security. The notification restricts the free flow of data by imposing data localization requirements on the payment system providers and limiting the cross-border transfer of payment data.

RBI's 2017 guidelines require Non-Banking Financial Companies (NBFCs) to maintain original records of offshore outsourcing activities in India and ensure that foreign regulatory authorities do not have access to data related to Indian operations simply because processing is conducted abroad.

Under the Companies Act, 2013, companies are required to maintain their books of account, other relevant documents, and financial statements at their registered office in India. An amendment to the Companies (Accounts) Rules, 2014, requires that all records maintained electronically must be accessible in India at all times, ensuring that critical financial data remains within Indian jurisdiction. Similarly, the Insurance Regulatory and Development Authority of India (IRDAI) mandates that insurers must store records related to policies, claims, and other related documents in data centers located within India. These rules restrict the free flow of data by imposing data localization requirements on the companies and limiting the storage of accounts and records in electronic mode outside India.

The Cyber Security Directions, 2022 by CERT-In are issued under the Information Technology Act, 2000 to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such data for lawful purposes and for matters connected therewith or incidental thereto. The directions mandate that the entire digital personal data shall be stored in systems located only in India, except for cross-border transactions where a copy of the domestic component may be stored abroad. The directions also prohibit the use of anonymous VPNs and require the data centres, VPS providers, cloud service providers and VPN service providers to validate the identity and address of their subscribers or customers. The directions also prescribe the minimum standards of data security and data breach reporting. The directions aim to augment and strengthen the cyber security in the country and safeguard the sovereignty, integrity, defence, security and public order of India. The directions restrict the free flow of data by imposing data localization requirements, banning anonymous VPNs and requiring identity verification of data users.

The Unified Access Licence by the Department of Telecommunications is a licence granted to the service providers to provide various telecom services such as basic, cellular, internet, national long distance, international long distance, etc., under a single licence. The licence contains various terms and conditions relating to the scope, duration, fees, obligations, quality of service, security, etc., of the licence. The licence also requires the licensee to provide necessary facilities for continuous monitoring of all traffic by the security agencies and to ensure that no encrypted messages are sent without the permission of the government. The licence also prohibits the licensee from transferring the customer information to any person or place outside India. The licence aims to provide a level playing field for the service providers and to ensure the security and integrity of the telecom network and services. The licence restricts the free flow of data by imposing surveillance obligations, encryption restrictions and data transfer prohibitions on the service providers.

Section 4 of the Public Records Act, 1993, prohibits any "public record" from being taken out of India without the prior approval of the Central Government. Since section 4 of the RTI Act obligates government agencies to upload public documents online, it may be assumed that insofar as the scope of the RTI Act is concerned, there is implicit approval to take the public documents disclosed under section 4, outside India.

The Securities and Exchange Board of India (SEBI) framework requires that all data, including logs and any other related information pertaining to SEBI-regulated entities, must be stored and processed within India. This rule ensures that original data, particularly concerning foreign investors, remains accessible within Indian borders. The SEBI advisory requires financial institutions using Software as a Service (SaaS) solutions to store critical data, such as risk and system information, within India.

The Consumer Protection (Direct Selling) Rules, 2021, under Rule 5(5), stipulate that direct selling entities must store "sensitive personal data" within Indian territory. The definition of

"sensitive personal data" is provided via reference to Section 43A of the Information Technology (IT) Act. But Section 43A of the IT Act has been repealed by the DPDP Act, 2023. So it is unclear what obligation direct sellers continue to have to locally store sensitive personal data.

Section 16(1) of the Digital Personal Data Protection Act, 2023 (DPDPA) gives the Central Government the power, by notification, to restrict the flow of personal data to specific countries that may be specified in the notification.

There are a number of other regulations such as the RBI Master Direction on KYC (regarding video KYC data),[57] Consolidated FDI Policy (regarding customer databases in broadcasting sector),[58] etc.

National Security and Law Enforcement

1. Information Technology Act, 2000
2. Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009
3. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
4. Information Technology (Guidelines for Cyber Cafe) Rules, 2011
5. Digital Personal Data Protection Act, 2023
6. Telecommunications Act, 2023
7. Model Police Manual, and States' Police Acts
8. Indian Telegraph Act, 1885 (now repealed)
9. Indian Post Office Act, 1898
10. The Bharatiya Nagarik Suraksha Sanhita, 2023 (replacing the Code of Criminal Procedure, 1973)

Various laws have provisions for surveillance and interception for law enforcement purposes, including Sections 69 and 69B of the Information Technology Act, 2000, and Section 20 of the Telecommunications Act, 2023 (replacing Section 5 of the Indian Telegraph Act, 1885). These provisions, along with the rules made thereunder, allow for interception of electronic communications and for compelled decryption of communications. Section 26 of the Indian Post Office Act, 1898, empowers the central and state government to intercept postal articles.

Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (which replaced the Code of Criminal Procedure, 1973) allows any court in India or any officer in charge of a police station to summon a person to produce any document or any other thing that is necessary for the purposes of any investigation, inquiry, trial or other proceeding. Section 95 allows for the interception of a document, parcel or thing in the possession of a postal authority. Surveillance procedures are also covered under various states' Police Acts and the national Model Police Manual.

Section 17(1)(c) of the Digital Personal Data Protection Act, 2023 exempts the application of the much of the law when "personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India". Section 17(2)(a) provides a wide-ranging exemption for "such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these." The government will presumably notify intelligence agencies under this provision.

---

[57] Master Direction - Know Your Customer (KYC) Direction, 2016, as amended in 2021.

[58] Consolidated FDI Policy, 2020, Annexure 6, Clause 1.3(ix).

3.2.2 Individual rights

1. Section 43A, Information Technology Act, 2000.
2. Digital Personal Data Protection Act, 2023.
3. Copyright Act, 1957
4. MCI's Code of Ethics Regulations, 2002
5. Credit Information Companies (Regulation) Act, 2005

Section 43A of the Information Technology Act, 2000 imposed civil liability on any 'body corporate' that dealt with 'sensitive personal data or information' and failed to maintain reasonable security practices and procedures to protect such data from unauthorized access, damage, use, modification, disclosure or impairment. The body corporate was made liable to pay damages by way of compensation to the person affected by such negligence. The Act defined sensitive personal data or information as any personal information that may be prescribed by the Central Government in consultation with professional bodies or associations. The Act restricted the free flow of data by imposing a duty of care and compliance on the data handlers and created a legal remedy for the data subjects. This provision will be repealed once the Digital Personal Data Protection Act, 2023 comes into force.

The Digital Personal Data Protection Act, 2023 provides for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such data for lawful purposes and for matters connected therewith or incidental thereto. The Act establishes a dedicated legal framework for data protection in India and defines the rights and duties of the data principals, data fiduciaries, data processors and the data protection board. The Act also lays down the principles and conditions for the collection, processing, storage, transfer, disclosure and deletion of digital personal data. The Act also provides for the penalties and remedies for any violation of the Act. The Act aims to protect the privacy and autonomy of the individuals and to promote the growth and innovation of the digital economy. The Act restricts the free flow of data by imposing consent and purpose limitations, data quality and security obligations, data protection impact assessments, data audits, data breach notifications and cross-border data transfer conditions on the data handlers.

The Copyright Act, 1957 protects original literary, dramatic, musical and artistic works and cinematograph films and sound recordings from unauthorized uses. The Act grants the authors and owners of such works exclusive rights to reproduce, publish, communicate, perform, adapt and translate their works for a limited period of time. The Act also provides for certain exceptions and limitations to the copyright protection, such as fair dealing, private use, educational use, etc. The Act also provides for the registration, assignment, licensing and transmission of copyright and the remedies for any infringement of copyright. The Act aims to encourage the creation and dissemination of intellectual and artistic works and to balance the interests of the authors, users and the public. The Act restricts the free flow of data by imposing legal restrictions on the copying, distribution, modification and use of the protected works without the permission or payment of the copyright holders. The Act doesn't address scraping for AI, though it provides a limited exception for "transient and incidental" usage of copyrighted materials, which would probably apply to search engines but might or might not be applicable to the collection of training data for AI models.

3.2.3 International agreements

The link between data governance and trade agreements isn't often clear. A scholar has observed that "most international trade agreements, especially the WTO treaties, were not designed to

address issues of the data-driven world."[59] Some scholars have argued that "the current approach in India in data governance and digital trade is largely nationalist and parochial."[60] But that opinion is contestable, given the push by India for global adoption of digital public infrastructure and digital public goods created in India, while basing those DPIs and DPGs on open standards and free/open source software developed internationally.

India's position on data governance with respect to trade agreements and Mutual Legal Assistance Treaties (MLATs) reflects its desire to assert its digital sovereignty and protect its data interests.[61] India has chosen not to join global initiatives such as the G20 Osaka Track Agreement on Data Free Flow with Trust and the WTO's Joint Statement Initiative on E-commerce, which advocate for free and open data flows. The country contends that these initiatives fail to sufficiently consider the developmental and regulatory priorities of developing nations, including data privacy, data security, data taxation, and data ownership.[62] Additionally, India has resisted including binding commitments on data flows in its trade agreements with countries like the US, the EU, and Japan. Instead, India favours more flexible, non-binding language that underscores the importance of data flows, acknowledges the right to regulate data, and promotes cooperation and dialogue on data issues.[63]

India has not adopted the Budapest Convention, which is the most widely accepted international framework for cooperation on cybercrime and electronic evidence. India has proposed an alternative approach to the UN Ad-hoc Committee on Cybercrime, which would grant countries a broader jurisdiction over data that is related to their citizens, irrespective of where the data is stored, processed, or accessed. "At the sixth session of the "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" held from August 21-September 1, India asked for the deletion of a clause encouraging state parties to "establish bilateral or multilateral arrangements" to facilitate the transfer of personal data… India also agreed to the clause that state parties may transfer personal data to a third country or an international organisation only with the prior written authorisation of the original transferring state party, subject to effective and appropriate safeguards."[64]

This approach would bypass the need for MLATs or data localization measures, which India considers to be inefficient and ineffective mechanisms for data sharing on criminal matters. As of 2021, "there were 845 pending requests from India with various countries under the Mutual Legal Assistance Treaty (MLAT) and other requests raised with foreign courts."[65]

---

59 Mishra, "Data Governance and Digital Trade in India."
60 Mishra.
61 Kedia et al., *Report |Governing Cross-Border Data Flows*.
62 Kedia et al.
63 Kedia et al.
64 Singh, "Transfer of Personal Data Under U.N. Treaty Will Be According to Native Laws."
65 Kedia et al., *Report |Governing Cross-Border Data Flows*.

4 In-depth : data protection and digital public infrastructure

In this section, we will take an in-depth look at two areas: data protection and 'India Stack', which has now evolved into India's 'Digital Public Infrastructure'.

4.1 Digital Personal Data Protection Act

Until very recently, data protection was a singular policy gap when it came to data governance in India. In 2023, with the passage of the Digital Personal Data Protection Act, that got addressed to an extent, but the law is yet to be brought into effect. The Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark legislation that aims to provide a comprehensive framework for the protection of digital personal data in India. The DPDP Act is the culmination of a long and arduous journey that spanned nearly two decades and involved various actors and stages. In this article, we will briefly trace the history of the DPDP Act and highlight some key milestones and challenges along the way

The idea of a data protection law in India dates back to 2006, when the first Private Member's Bill on data protection was introduced in the Parliament. However, the Bill did not receive much attention or support, and eventually lapsed. In 2008, the government amended the Information Technology Act to insert section 43A, a provision on 'reasonable security practices'. The key elements of Section 43A were:

- Data Protection Obligations: If a body corporate possessing, dealing, or handling sensitive personal data or information in a computer resource is negligent in implementing and maintaining reasonable security practices, resulting in wrongful loss or gain to any person, the body corporate is liable to pay damages.
- Liability for Negligence: The section places a legal obligation on organizations to exercise due diligence in protecting sensitive personal information and holds them accountable for any negligence leading to harm.

In 2012, rules were framed under Section 43A providing more detailed guidelines. These rules are known as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Key provisions of these rules include:

- Reasonable Security Practices: The rules define what constitutes "reasonable security practices" and lay down the standards that organizations are expected to follow to safeguard sensitive personal data.
- Definition of Sensitive Personal Data: The rules provide a comprehensive definition of "sensitive personal data or information," encompassing various categories such as passwords, financial information, health records, sexual orientation, and biometric data.
- Data Breach Notification: The rules specify the obligations of organizations in the event of a data breach, emphasizing the need for prompt notification to affected individuals and relevant government authorities.
- Adjudicating Officer: The rules establish the role of an adjudicating officer to hear and adjudicate claims arising from the breach of data protection obligations. This officer has the authority to award damages to affected parties.

Civil society played an important part, as did Aadhaar, in making privacy a broader part of the discourse in India. Aadhaar, India's national unique identity project, raised several concerns regarding the collection, storage, and use of biometric and demographic data of millions of Indians, and sparked a series of debates and litigations on the right to privacy and data protection.

In the early 2000s various civil society groups started working on privacy and advocating for a data protection law, apart from organizing events and bringing people together on the importance and urgency of safeguarding the rights and interests of data subjects in the digital age. In 2010, the Government of India released a "Privacy Approach" paper, which outlined the basic principles and objectives of a privacy framework for India. The paper invited comments and feedback from the public and the stakeholders, but did not propose any concrete draft or bill. In 2011, CIS obtained and leaked a draft of the "Privacy Bill, 2011", which was prepared by the Department of Personnel and Training (DoPT) and circulated among some ministries and departments. The draft bill was based on the "Privacy Approach" paper, but also included some provisions and clauses that were problematic or controversial. In 2012, the Government of India constituted a Group of Experts on Privacy under the chairmanship of Justice A.P. Shah, a former Chief Justice of the Delhi High Court. The Group submitted its report in October 2012, which recommended a set of nine privacy principles and a draft outline of a privacy bill.

4.1.1 Gained pace in the last decade

In 2013, CIS, a civil society organization, put together a "citizens' draft" of a "Privacy (Protection) Bill, 2013", which was based on the Justice Shah Group's report and international best practices. In collaboration with two industry bodies, FICCI and the Data Security Council of India, they held extensive consultations across seven meetings with civil society, government. The draft bill was submitted to the DoPT and the Planning Commission, but did not receive any official response or acknowledgement.

In 2017, the Supreme Court of India delivered a historic judgment in the case of *Puttaswamy v. Union of India*, which re-affirmed that privacy is a fundamental right under the Constitution of India. The judgment also directed the Government of India to enact a data protection law as soon as possible, and to constitute a committee of experts to draft the law. In 2018, the Save our Privacy campaign, a collective of civil society organizations and individuals, launched the 'Indian Privacy Code, 2018', which was a model bill for data protection and surveillance reform in India. The campaign also initiated a petition and a letter campaign to urge the Government of India to adopt the bill.

4.1.2 Five years of government drafts

In 2018, the Government of India appointed a Committee of Experts on a Data Protection Framework under the chairmanship of Justice B.N. Srikrishna, a former Supreme Court judge. The Committee submitted its report and a draft bill, titled the "Personal Data Protection Bill, 2018", in July 2018. The draft bill was based on the Supreme Court's judgment and the global and regional standards and developments in data protection. The draft bill was also made public for comments and suggestions from the stakeholders and the public.

However, the draft bill was not introduced in the Parliament in 2018, and was instead revised and modified by the Government of India. The revised draft bill, titled the "Personal Data Protection Bill, 2019", was introduced in the Lok Sabha in December 2019. The draft bill was referred to a Joint Parliamentary Committee (JPC) for further examination and consultation.

The draft bill faced several criticisms and controversies, as it introduced some changes and additions that were seen as diluting or deviating from the original draft bill and the Supreme Court's judgment.

The JPC did not submit its report or recommendations on the draft bill in 2019, and sought several extensions and adjournments. Finally, in 2021, the report of the JPC was tabled in Parliament, along with a revised draft bill prepared by the JPC, titled the "The Data Protection Bill, 2021", which was also intended to regulate non-personal data. In 2022, the government made available for public consultation a "Draft Digital Personal Data Protection Bill, 2022". The comments received were not published by the government.

In August 2023, the "Digital Personal Data Protection Bill, 2022" was introduced in the Lok Sabha. The Bill was passed by both the Houses of the Parliament in August 2023, and received the President's assent that same month. This law differs significantly from all the previous versions.

4.1.3 Frictions and trade-offs between policies and policy objectives

When it comes to the DPDP Act, the trade-offs have not been clearly articulated since it was not accompanied by a whitepaper — unlike the Srikrishna Committee's draft of the Personal Data Protection Bill, 2018 — nor a detailed statement of objects & reasons. So one can only surmise the trade-offs considered by the policymakers based on the text of the law, the revisions made since the previous drafts of the data protection law, and also the differences from other international benchmarks such as the EU's GDPR. One way to look for trade-offs is to look at the prominent debates in public fora such as newspapers.

The most prominent of these debates that accompanied the DPDP Bill was that relating to the balancing of privacy and transparency, specifically as relates to the Right to Information Act.[66]

Prior to the passage of the DPDP Act, Section 8(1)(j) of the RTI Act provided a balancing test between transparency and privacy, which stated:

> Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information: Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person.

This provision was substituted by the DPDP Act, with a provision that simply stated:

> Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen information which relates to personal information.

---

[66] *The Hindu*, "Data Protection Bill Poses Severe Restrictions to RTI Act, Advocacy Group NCPRI Cautions Government"; *The Wire*, "'Regressive Amendments to RTI Act'"; *Financial Express*, "Short Shrift for RTI; Public Interest Should Not Be Harmed by Denial of Information."

This clearly privileges confidentiality of personal information over the right to information, rather than seeking to optimize the trade-off between personal data protection and transparency. During the parliamentary debate over the DPDP Act, multiple opposition Members of Parliament mentioned the criticisms levelled by transparency activists, but the government did not address any of these criticisms.

One other way to look for trade-offs is to examine what gets covered by the law and what doesn't — via the definitions, the protections afforded, the exemptions, and so on.

- Applicability: Unlike the GDPR, the Indian DPDP Act doesn't apply to non-digital data. This leaves all existing paper records out of its ambit, while including them as and when they are digitized. This reduced scope simplifies things by excluding many quotidian cases of personal data use, without causing much harm, since the potential for data-oriented harm — as opposed to, say a tort like breach of confidentiality — arising from non-digital data is non-existent. Thus, there isn't much of a trade-off by excluding non-digital data from the scope of the law. Another reduction in scope is the law confining the term "processing" to mean only *wholly or partly automated* operations, whereas laws such as the GDPR include both automated and non-automated processing of data. This potentially has tremendous ramifications, which I am not clear the policymakers have fully understood since some of the examples that they provide in the law seem to include non-automated processing.
- Extraterritorial applicability: The law is extraterritorial in its applicability, applying even in cases where processing is "in connection with any activity related to offering goods or services to Data Principals within India". In this regard, it follows India's Information Technology (IT) Act and the EU's GDPR, both of which provides for extraterritorial applicability. Extraterritorial applicability brings with it difficulties of enforcement — what if a company processes data of Indians, but those data principals are unable to sue the company in India, or enforce any judgment against it in India, since it doesn't have any legal representatives in India? But the main solution to this — requiring appointment of legal representatives in one's territory — creates an extremely high barrier to operation in a borderless digital world. The policymakers seems to have opted for a *via media* — certain "significant data fiduciaries", which deal with large volumes of data about Indians (how much is yet to be specified), will need to appoint data protection officers in India.
- Categorization of data: While earlier versions of the data protection law had multiple categories of personal data, including "sensitive personal data" and "critical personal data" — health data being covered by the latter — the DPDP Act does not. This seeks to trade-off (arguably necessary) complexity for ease of enforcement.
- Cross-border sharing of data: The Act does not provide any guidance on the cross-border transfer of personal data, especially in relation to the adequacy of data protection regimes in other countries. It provides for the government to create a negative list of countries to which data may not be transferred. This is, of course, difficult to enforce since a data fiduciary in a foreign country may transfer data to a blacklisted country, and this becomes very difficult to monitor and thereupon to remedy that. There is also no indication on what considerations would be taken into account when drawing up the negative list, perhaps the Legislature wanted to give the government leeway in drawing up this list so that the ever changing conditions of international geopolitics could be taken into account.
- The Act does not address the issue of data localization, which may have implications for the competitiveness and innovation of the digital economy, as well as for law enforcement and national security. However it must be noted that there may be data localisation requirements

imposed through other legislations and regulations such as RBI circulars in the financial sector, or the Telecommunications Act, 2023.

- The Act does not establish a clear mechanism for the coordination and cooperation between the Data Protection Board and other sectoral regulators, such as the Reserve Bank of India, the Telecom Regulatory Authority of India, and the Securities and Exchange Board of India.
- Rights of data principals
  - Unlike the GDPR, the DPDP Act does not provide a right to data portability (though this was there in the 2019 Bill), a right to object to processing based on other grounds than consent, and the right not to be subject to solely automated decision-making. Instead, The DPDP Act provides for two other rights: the right to "grievance redressal," which ensures that data principals have an easily accessible contact point provided by the data fiduciary to handle complaints, and the right to "appoint a nominee," allowing the data principal to designate someone to exercise their rights in the event of their death or incapacity.[67]
  - The rights of access, erasure, and correction as well as notice of data collection are restricted to personal data processing based on explicit consent or "voluntary disclosure" (implicit consent) for legitimate use. This means that government bodies or other fiduciaries utilizing any "legitimate uses" grounds are not obligated to respond to access or erasure/correction requests, unless further rules enacted by the government specify otherwise. This is a gigantic departure from the GDPR.
  - Even in a right that is common between the GDPR and the DPDP Act — such as the right of access — the scope is quite different. Under the DPDP Act, this right allows data principals to request and obtain a summary of the personal data being processed and relevant processing activities, rather than a copy of the personal data. It also includes the identities of all fiduciaries and processors with whom the personal data has been shared, along with a summary of the data shared. However, Section 11 of the Act leaves room for future rules that may specify additional information to be provided.
  - As under the GDPR, under the DPDP Act, data principals can request the erasure of personal data under Section 12(3), and erasure may also be required automatically after consent withdrawal or when the specified purpose is no longer served (Section 8(7)(a)). Similarly, correction, completion, and updating of personal data can be requested by the principal and must occur automatically when the data is likely to be used to make a decision affecting the principal (Section 8(3)).

Thus, there are many restrictions in the rights of data principals, which would arguably make the law easier to administer for corporations and the government. The Act also has a section on duties of data principals, something which is not seen in laws such as the GDPR.

There are also a number of exemptions from the law:

- For notified agencies, in the interest of security, sovereignty, public order, etc.
- For research, archiving, or statistical purposes.
- For notified categories of data fiduciaries, including start-ups.
- To enforce legal rights and claims.
- To perform judicial or regulatory functions.
- To prevent, detect, investigate, or prosecute offences.

[67] Roy and Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained - Future of Privacy Forum."

- To process in India personal data of non-residents under foreign contracts.
- For approved merger, demerger, etc.
- To locate defaulters and their financial assets, etc.

These are mostly oriented towards safeguarding collective interests such as security objectives, governmental functioning, and research interests, against the individualistic interests that data protection seeks to safeguard. It is possible that the exclusion of processing data of non residents has been made to safeguard the interests of the IT industry in India, by lowering the compliance burden on it.

4.1.4 Openness of policy development process

The policy development process of the DPDP Act, 2023 has been a paradoxical mix of openness and opacity, as it involved multiple rounds of public consultations, but also several revisions and modifications that were not based on the public or the stakeholders' inputs, and were not made public or transparent. In this article, we will analyze how the policy development process has been incredibly open and incredibly opaque at the same time.

On the one hand, the policy development process has been incredibly open, as it provided various opportunities and platforms for the public and the stakeholders to participate and contribute to the drafting and the consultation of the data protection law. The policy development process started with a bottom-up and participatory approach, as civil society organizations and individuals initiated and advocated for a data protection law, and prepared and submitted their own draft bills and model codes, such as the "Privacy (Protection) Bill, 2013" and the "Indian Privacy Code, 2018". The policy development process also involved a top-down and consultative approach, as the Government of India constituted various committees and groups of experts to draft and report on a data protection framework, such as the Justice Shah Group of Experts and the Justice Srikrishna Committee of Experts. These committees and groups consulted with various stakeholders, such as the Government, the industry, the civil society, the academia, and the international organizations, and invited comments and feedback from the public and the stakeholders on their draft bills and reports.

The draft bills were also examined and scrutinized by a Joint Parliamentary Committee (JPC), which is a representative committee of the members of both the Houses of the Parliament. The JPC also held several hearings and meetings with various stakeholders, such as the Government, the industry, the civil society, the academia, and the international organizations, and sought their views and suggestions on the draft bills.

On the other hand, the policy development process was incredibly opaque and unresponsive in the end, as it involved several revisions and modifications that were not based on the public or the stakeholders' comments and suggestions. The Digital Personal Data Protection Bill, 2023, was not accompanied by a paper explaining why changes were made since the previous version of the Bill, nor were stakeholder comments made public. Hence, one could only speculate as to why various data principals' rights were removed or restricted. Further, the law was rushed through Parliament after it was introduced, without providing responses to any of the concerns raised by various Members of Parliament.

Therefore, the policy development process of the DPDP Act, 2023 has been a contradictory process, that has exhibited both the elements of openness and opacity.

4.1.5 Capacity challenges

Until the law is actually enforced, the capacity challenges cannot be accurately mapped. However, one can make some preliminary observations. The 2018 draft of the Data Protection Bill proposed by the Srikrishna Committee envisioned an all-powerful Data Protection Authority having much more powers than even DPAs under the GDPR. By contrast, the DPDP Act envisions a far more limited Data Protection Board (DPB) that has fewer powers and is directly under the control of the government. The DPB has the power to investigate complaints and issue penalties, but does not have the power to make regulations or issue any codes of conduct. Appeals from the DPB, quite strangely, lie to the Telecom Dispute Settlement and Appellate Tribunal. The state capacity challenges that would have been a concern with the previous iterations of the data protection law are not there, but the opposite concern now arises: whether the DPB has sufficient powers to oversee the enforcement of the fledgling data protection law.

In terms of compliance by governments and businesses, it is important to note that the DPDP Act, unlike the GDPR, applies only to digital personal data — data that's either been digital from the start or digitized. It doesn't apply to paper records. This eases the compliance burden a little, and thus reduces the state capacity requirements.

4.2 India Stack, Digital Public Infrastructure, and Digital Public Goods

India Stack is the name given to a set of initiatives by various Indian government departments and agencies along with private players (like iSPIRT) that aim to transform the data governance landscape in India. India Stack is "a set of APIs and digital public goods" that allows governments, businesses, startups and developers to utilise and engage in presence-less, paperless, and cashless service delivery.

India Stack initially consisted of three layers: identity, payments, and data and consent. The identity layer provides a digital identity to every Indian citizen through Aadhaar, a biometric-based unique identification system. The payments layer enables real-time digital payments through UPI, a unified payments interface that connects multiple bank accounts and payment platforms. The data and consent layer facilitates the creation and exchange of digital documents and records through eSign, eKYC, and DigiLocker. The Data Empowerment And Protection Architecture (DEPA) allows users control over their own data, with the ability to access and share their data through third-party entities called Consent Managers. The Consent Managers are intermediaries that provide an interface to facilitate the easy sharing and consumption of data from various entities with user consent. As per the provisions of the Digital Personal Data Protection Act, 2023, such Consent Managers have to be registered with the Data Protection Board of India and be accountable to the data principal and also be subject to any Rules that may be made in regard to their obligations under the DPDP Act, 2023 including providing a grievance redressal mechanism to the data principal.

The electronic consent artefact is a standardized and programmable digital template for capturing user consent to share their personal data with third parties. DEPA has been implemented in the financial sector under the Account Aggregator framework, which allows users to access and share their financial data across different institutions, such as banks, insurance companies, mutual funds, and tax authorities. DEPA is also being tested in the health sector, where users can access and share their health records and prescriptions with doctors,

hospitals, and pharmacies. DEPA is expected to be extended to other sectors, such as education, agriculture, and telecom.

Although it has now become a part of India's official and dominant model of digital transformation, India Stack started as an initiative of a think tank of the Indian IT Industry, iSPIRT. The Aadhaar project paved the way for a vision of an interconnected grid of information infrastructures consisting of a universal ID for each citizen, allowing for electronic flow of funds and direct benefit transfers to bank accounts. The India Stack designers built upon this vision to facilitate entrepreneurship by allowing private players to build businesses around different layers of digital infrastructure.[68] The institutions involved in developing and operating India Stack enjoy state policy backing to expand market access while at the same time escaping regulatory oversight because they are not 'state'. Such a system also allows the state to distance itself from failures and evade accountability for addressing challenges to improve development.[69]

To some extent, Aadhaar has succeeded in eliminating inefficient practices in welfare delivery. For example, ration cards were issued at state level and therefore, it was difficult for migrant workers to use it in their state of work. Schemes like "One nation, one ration card" which linked state issued ration cards to Aadhaar, definitely helped in making the system more efficient. The problem comes from Aadhaar's function creep. Failure to define the scope and boundaries of Aadhaar's application has led to it being embedded as a de-facto universal ID and an authentication tool.[70]

Despite the success of certain parts of the Aadhaar project and India Stack (e.g., UPI), there are limitations and criticisms which centre primarily on issues such as accountability, transparency and openness. There is limited knowledge of, and transparency in the development of the centralised APIs. The participation of volunteers and their mandates was also decided behind closed doors as India Stack is neither bound by procurement prohibitions nor are their actions auditable. This arrangement means India Stack operates without the same degree of oversight mandated by similar government projects.[71] While it may offer certain advantages in terms of reducing inefficiencies of government-owned systems, it throws up issues of competition and governance owing to the lack of accountability in the functioning of such entities.[72]

Questions have also been raised about the 'open' credentials of India Stack due to the lack of benchmarks to define what openness is and how it is to be assessed, leading to concerns about open washing, i.e., describing something as 'open' when it is in fact not.[73] Looking at the vast data collection practices of Aadhaar and India Stack, commentators have also raised issues such as 'governtrepreneurship', (weaving of corporate into government thus complicating the relationship between state, corporates and the populations)[74] as well as data colonialism.[75]

The framing of India Stack as "Digital Public Infrastructure" enables the state to continue to act as an investor, providing funding or subsidising costs. The state embeds India Stack products and services across various aspects of the digital economy not just with the aim of propelling innovation or addressing socio-economic challenges. Rather, as these services scale, they become

---

68 Parsheera, "Stack Is the New Black?"
69 Panday, *India Stack*, 91.
70 Panday, *India Stack*.
71 Parsheera, "Stack Is the New Black?"
72 Parsheera.
73 Parsheera.
74 Dattani, "'Governtrepreneurism' for Good Governance."
75 Dattani, "Spectrally Shape-Shifting."

sources to attract foreign investment, as is evident in the state acting as a promoter, marketing India Stack for export to other countries through various forums.[76] Promoting India Stack under the broader concept of DPI was an important element in the Indian government's presidency of the G20. Under India's leadership, the G20 Economic Ministers produced an outcome document in which a working definition of "digital public infrastructure" was given as "a set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications", whose aims were "to deliver and provide equitable access to public and / or private services at societal scale" and whose governance is through "applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms."[77]

The government has listed the following as part of India's "digital public infrastructure"

- Aadhaar (biometric-based digital identity)
- Unified Payments Interface (payments system)
- DigiLocker (credentials storing and sharing)
- Umang (gateway app for government services)
- eSanjeevani (tele-medicine service)
- API Setu (API directory)
- Co-WIN (vaccination system)
- Government eMarketplace (platform bringing together governments and vendors)
- Diksha (education)

India has also pushed for the idea of "digital public goods" at the UN level through non-state actors which have received state backing in the past. EkStep, an Indian non-profit co-founded by those who conceptualized Aadhaar, is on the board of the Digital Public Goods Alliance,[78] whereas Indian entities like eGov Foundation and iSPIRT are among the members. This shows India's eagerness to push the concepts of 'Digital Public Infrastructure' and 'Digital Public Goods' internationally, while adopting international open standards. This seems to suggest that the narrative that India is being very nationalistic in terms of data governance are not all that correct.

4.2.1 Policy development processes

One of the biggest complaints of tech policy NGOs in India has been the hijacking by private organizations of the policy development process for all of India Stack. Private entities like the volunteer-based non-profit iSPIRT are seen as having captured both the policy development process as well as the tech development process for India Stack. This, critics argue, has led to opacity and lack of public participation in what are large-scale projects affecting hundreds of millions of people.

[76] Panday, *India Stack*, 91.
[77] *G20 Digital Economy Ministers Meeting: Outcome Document and Chair's Summary*, para 6.
[78] Digital Public Goods Alliance, "Governance."

5 Findings

5.1 Gaps

While laws and/or policies exist in India on most of the issues discussed in this paper such as open data, right to information, open-source software, copyright, data protection, etc. there are significant gaps when it comes to their actual implementation and enforceability, specially in light of recent policy developments in the global scenario. Some of the significant policy gaps identified in this paper are encapsulated below:

- India lacks robust laws on open standards, open access to scholarly literature, open-source software, and open government data. Although policies exist in all of the above areas, the current policies have neither been very successful in their implementation nor can they be enforced against the government.
- The RTI machinery in India suffers from various problems such as lack of political will, inadequate infrastructure, high levels of vacancy and backlog, poor record management, insufficient training, etc. Information seekers, especially marginalized groups, face a number of problems such as low awareness, inconsistent rules, uncooperative PIOs, and even intimidation, leading to poor quality responses and a lack of confidence in the system. These issues collectively undermine the potential of the RTI Act to promote transparency and accountability.
- India's recent data protection law is currently in limbo — the statute having been notified, but the rules to operationalize the Act, including the creation of a data protection board, not yet having been framed. This is a huge failure given all the personal data being collected by the government and corporations, especially with projects like UPI, Digilocker, and the various other DPIs. Further, even the statute itself has very limited protection for user rights, with wide-ranging exceptions of use of personal data by the state, and also overly strict grounds for processing of personal data (for instance, by not having a general 'legitimate interest' ground like the GDPR does).
- There are domains where the usage of open standards — such as Akoma Ntoso for laws, judgments, parliamentary debates, and so on — would greatly benefit the government, yet they are not being used.
- India's copyright law doesn't address scraping for AI, though it provides a limited exception for "transient and incidental" usage of copyrighted materials, which would probably apply to search engines but might or might not be applicable to the collection of training data for AI models.
- India's data protection law seems to put a complete bar on web scraping for any purpose, including search engines and machine learning. Only "publicly available personal data" that's been made or caused to be made publicly available by the data principal or under the law is exempted. It is impossible when scraping petabytes of data, to figure out whether there's personal data included in it and whether that personal data has been made available by the data principal or under the law. Unless there are rules framed that provide an exemption, inclusion of personal data, including from websites like Wikipedia, for the purposes of use in training of AI models seems to be prohibited.

5.2 Friction / Trade-offs

Due to its very nature there are bound to be various trade-offs in the realm of data governance —between privacy, transparency, national security, economic development, etc. As the objectives of these governance frameworks often clash, their handling is of particular interest to understand the issues that the state prioritises in its policy thinking. Some of the trade-offs in data governance and how they have been handled are mentioned below.

- In some cases, such as the Government Open Data Licence (GODL), or the DPDP Act, conformity to existing laws is explicitly considered. The GODL, e.g., excludes personal information from the scope of the licence, along with information of the categories listed under Section 8 of the RTI Act, showing that trade-offs were considered, and a cohesive approach was followed, with references to existing laws. Similarly, the DPDP Act makes references to other laws such as the Rights of Persons with Disabilities Act, allowing guardians of persons with disabilities, if they've been appointed one by a court, to provide and manage consent on behalf of the person with disability. This again shows that friction between laws has been sought to be addressed.
- **Privacy vs. Transparency:** Whenever census or survey data is published, the perennial concern is the trade-off between data accuracy and utility versus privacy. Indian laws seek to explicitly negotiate that trade-off by ensuring that individual-level privacy is maintained at all times. However, as far as the DPDP Act is concerned, it clearly gives a priority to privacy over transparency by making personal privacy a blanket exception in the right to information law.
- **Extraterritorial applicability vs. Enforcement:** Extraterritorial applicability brings with it difficulties of enforcement — since the company may not have any physical presence in India, and the main solution to this — requiring appointment of legal representatives in India — creates an extremely high barrier to operation in a borderless digital world. The policymakers seems to have opted for a *via media* — certain "significant data fiduciaries", which deal with large volumes of data about Indians, will need to appoint data protection officers in India.
- **Rights of data principals vs. Ease of operations:** Although data principals have been give a number of rights under the DPDP Act, there are many restrictions on these rights, e.g., reduced scope of the right to access, no right to data portability, etc., which would arguably make the law easier to administer for corporations and the government.
- **Interoperability vs. Innovation:** The push for the Open Network for Digital Commerce (ONDC) may adversely affect major marketplaces like Amazon and Flipkart, potentially harming innovation, though this aspect has not been widely debated. Like in the EU, standards-driven interoperability is being pushed. While this is eminently desirable, there ought to be public debate and discussion on the potential (and potentially unintended) consequences of interoperability.

5.3 Good Practices

- Successful implementations such as India Stack/Unified Payments Interface (UPI), despite their shortcomings (some of which have been discussed in this report).
- Institution-level mandates for open access.
- A strong right to information law, despite a tendency by the government to try to frustrate its implementation.
- Existence of a number of policies on FOSS, open standards and interoperability.

- Passing a data protection legislation after so many years, even if with a number of problems

5.4 Policy Development Challenges

The policy development process of the DPDP Act, 2023 was in some ways indicative of larger problems. That process was characterized by a paradoxical blend of transparency and obscurity. While it involved multiple rounds of public consultations and opportunities for stakeholder input, including bottom-up initiatives from civil society and top-down expert committees, the final stages of the process were marked by opacity. The government invited public participation through various platforms and even established a Joint Parliamentary Committee to examine draft bills.

However, the process ultimately became unresponsive and opaque, with several revisions and modifications made without clear explanations or consideration of public input. The final version of the Digital Personal Data Protection Bill, 2023, lacked transparency in its changes, and the law was rushed through Parliament without addressing concerns raised by MPs. This contradictory approach, combining elements of openness and opacity, has defined the policy development process of the DPDP Act, 2023.

Apart from this, the immense size of India leads to additional challenges, including:

- Issues related to federalism and subsidiarity.
- Understaffed civil services and a lack of qualified personnel.
- Tension between private firms and civil society, as happened in the case of India Stack.

References

Abraham, Sunil, and Vidushi Marda. *Free and Open Source Software (FOSS) and Open Standards*. No. 2. Economic, Social and Cultural Rights in India: Opportunities for Advocacy in Intellectual Property Rights. Association for Progressive Communications, 2016. https://cis-india.org/openness/files/economic-social-and-cultural-rights-in-india-foss/.

Agarwal, Natasha. "India Must Do More to See Impact of Open Data." General. *World Wide Web Foundation*, November 16, 2015. https://webfoundation.org/2015/11/india-must-do-more-to-see-impact-of-open-data/.

Central Statistics Office. *Handbook on the Collection of Statistics Act, 2008*. 2008. https://web.archive.org/web/20240701094806/https://www.mospi.gov.in/sites/default/files/main_menu/handbook_%2520collection_of_statistic_act/hand_col_stat_act_2008.pdf. https://www.mospi.gov.in/sites/default/files/main_menu/handbook_%20collection_of_statistic_act/hand_col_stat_act_2008.pdf.

Centre for Development of Advanced Computing. "C-DAC Free/Open Source Software." 2018. https://web.archive.org/web/20231116070519/https://cdac.in/?id=st_oss_free_open_source_software. https://cdac.in?id=st_oss_free_open_source_software.

Centre for Law and Democracy, and Access Info Europe. *Global Right to Information Rating*. Center for law and democracy, 2023. https://web.archive.org/web/20240812115711/https://www.rti-rating.org/rating/. https://www.rti-rating.org/rating.

Consolidated FDI Policy, 2020. Accessed December 8, 2024. https://static.investindia.gov.in/2020-10/FDI-PolicyCircular-2020.pdf.

Dattani, Kavita. "'Governtrepreneurism' for Good Governance: The Case of Aadhaar and the India Stack." *Area* 52, no. 2 (2020): 411–19. https://doi.org/10.1111/area.12579.

Dattani, Kavita. "Spectrally Shape-Shifting: Biometrics, Fintech and the Corporate-State in India." *Journal of Cultural Economy* 17, no. 4 (2024): 470–88. https://doi.org/10.1080/17530350.2023.2176340.

Dey, Nikhil, and Aruna Roy. "India in Open Government and Open Government in India." *Stanford Social Innovation Review* 11 (2013): A14. https://doi.org/10.48558/MB23-6H82.

Digital Public Goods Alliance. "Governance." Digital Public Goods Alliance - Promoting Digital Public Goods to Create a More Equitable World, November 25, 2021. https://web.archive.org/web/20240304203117/https://digitalpublicgoods.net/governance/. https://digitalpublicgoods.net/governance/.

Financial Express. "Short Shrift for RTI; Public Interest Should Not Be Harmed by Denial of Information." August 18, 2023. https://www.financialexpress.com/opinion/short-shrift-for-rti-public-interest-should-not-be-harmed-by-denial-of-information/3214133/.

G20 Digital Economy Ministers Meeting: Outcome Document and Chair's Summary. G20, 2023. https://web.archive.org/web/20240309092929/https://www.g20.in/content/dam/gtwenty/gtwenty_new/document/G20_Digital_Economy_Outcome_Document%2520_and_Chair's_Summary_19082023.pdf. https://www.g20.in/content/dam/gtwenty/gtwenty_new/document/G20_Digital_Economy_Outcome_Document%20_and_Chair%27s_Summary_19082023.pdf.

Government Open Data Licence (2017). https://data.gov.in/sites/default/files/Gazette_Notification_OGDL.pdf.

Hariharan, Venkatesh. "Open Standards Policy in India: A Long, but Successful Journey." Opensource.com, November 19, 2010. https://web.archive.org/web/20230711170320/https://opensource.com/government/10/11/open-standards-policy-india-long-successful-journey. https://opensource.com/government/10/11/open-standards-policy-india-long-successful-journey.

Information Technology Policy of Assam (2009). https://dispur.nic.in/itact/it-policy-assam-2009.pdf.

Jha, Rama Nath, Sarah Nazamuddin Harniswala, and Brij Bhushan Singh. *State Transparency Report*. No. 4. Transparency International India, 2020. https://transparencyindia.org/wp-content/uploads/2020/10/STR-Final-2020.pdf.

Kedia, Mansi, Mira Burri, Yik Chan Chin, and Susan Ariel Aaronson. *Governing Cross-Border Data Flows: International Trade Agreements and Their Limits*. Oxford Global Society, 2023. https://web.archive.org/web/20231120021028/https://oxgs.org/2023/04/12/governing-cross-border-data-flows-international-trade-agreements/. https://oxgs.org/2023/04/12/governing-cross-border-data-flows-international-trade-agreements/.

Kishan Chand Jain v. Union of India, 2023 INSC 741 ___ (2023).

Krishnaswamy, Girija, and Dora Marinova. "Free and Open Source Software (FOSS) in Education: IT@School Project, Kerala Region of India." *Journal of Free Software & Free Knowledge* 1, no. 1 (2012). https://web.archive.org/web/20231117201741/https://espace.curtin.edu.au/handle/20.500.11937/14340. https://espace.curtin.edu.au/handle/20.500.11937/14340.

Loney, Matt. "India Shares Open-Source Experience." *ZDNET*, September 24, 2004. https://web.archive.org/web/20231117190044/https://www.zdnet.com/article/india-shares-open-source-experience/null/. https://www.zdnet.com/article/india-shares-open-source-experience/.

Master Direction - Know Your Customer (KYC) Direction, 2016. Accessed December 8, 2024. https://www.rbi.org.in/scripts/bs_viewmasdirections.aspx?id=11566#21.

Matthan, Rahul, and Shreya Ramann. "India's Approach to Data Governance." In *Data Governance, Asian Alternatives: How India and Korea Are Creating New Models and Policies*, edited by Evan A. Feigenbaum and Michael R. Nelson. 2022. https://web.archive.org/web/https://carnegieendowment.org/2022/08/31/india-s-approach-to-data-governance-pub-87767. https://carnegieendowment.org/2022/08/31/india-s-approach-to-data-governance-pub-87767.

Ministry of Electronics and Information Technology. "API Setu." 2020. https://web.archive.org/web/20231113155453/https://www.meity.gov.in/api-setu. https://www.meity.gov.in/api-setu.

Ministry of Electronics and Information Technology. "Major FOSS Initiatives." September 27, 2021. https://web.archive.org/web/20231116034239/https://www.meity.gov.in/content/major-foss-initiatives. https://www.meity.gov.in/content/major-foss-initiatives.

Ministry of Electronics and Information Technology. "Open Government Data (OGD) Platform India." January 21, 2022. https://web.archive.org/web/20230711164605/https://data.gov.in/. https://data.gov.in.

Mishra, Neha. "Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?" In *Data Sovereignty: From the Digital Silk Road to the Return of the State*, edited by Anupam Chander and Haochen Sun. Oxford University Press, 2023. https://web.archive.org/web/

20240628130329/https://academic.oup.com/book/55328/chapter/428798735. https://doi.org/10.1093/oso/9780197582794.003.0011.

Narasimhan, Nirmita, Mukesh Sharma, and Dinesh Kaushal. *Accessibility of Government Websites in India: A Report*. 2012. https://web.archive.org/web/20231111053416/https://cis-india.org/accessibility/accessibility-of-govt-websites.pdf. https://cis-india.org/accessibility/accessibility-of-govt-websites.pdf.

National Data Sharing and Accessibility Policy (2012). https://data.gov.in/sites/default/files/NDSAP.pdf.

National Geospatial Policy (2022). https://www.surveyofindia.gov.in/webroot/UserFiles/files/National%20Geospatial%20Policy.pdf.

National Informatics Centre. "Guidelines for Indian Government Websites and Apps 3.0." May 17, 2023. https://web.archive.org/web/20231111071229/https://guidelines.india.gov.in/. https://guidelines.india.gov.in/.

National Informatics Centre. "SugamyaWeb." 2024. https://sugamyaweb.gov.in/landing/using-sugamyaweb.html.

National Policy on Information Technology (2012). https://www.meity.gov.in/writereaddata/files/National_20IT_20Policyt%20_20.pdf.

National Policy on Software Products (2019). https://www.meity.gov.in/writereaddata/files/national_policy_on_software_products-2019.pdf.

OECD. *Going Digital Guide to Data Governance Policy Making*. OECD, 2022. https://web.archive.org/web/20231116075558/https://www.oecd-ilibrary.org/science-and-technology/going-digital-guide-to-data-governance-policy-making_40d53904-en. https://doi.org/10.1787/40d53904-en.

OGD Division, NIC. *Implementation Guidelines for NDSAP*. 2015.

"ONDC Project." April 6, 2022. https://web.archive.org/web/20230829040854/https://pib.gov.in/Pressreleaseshare.aspx?PRID=1814143. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1814143.

Open Access Mandate (2011). http://www.csircentral.net/mandate.pdf.

"Open Geospatial Data from Government of India - OpenStreetMap Wiki." https://web.archive.org/web/20230724073537/https://wiki.openstreetmap.org/wiki/Open_Geospatial_Data_from_Government_of_India. Accessed July 24, 2023. https://wiki.openstreetmap.org/wiki/Open_Geospatial_Data_from_Government_of_India.

Panday, Jyoti. *India Stack: Public-Private Roads to Data Sovereignty*. Internet Governance Project, 2023. https://www.internetgovernance.org/wp-content/uploads/India_stack_9_1_2023.pdf.

Panjiar, Tejasi, and Prateek Waghre. "A Comparison of State-Level Data Policies." Internet Freedom Foundation, June 4, 2022. https://web.archive.org/web/20231113162032/https://internetfreedom.in/a-comparison-of-state-level-data-policies/. https://internetfreedom.in/a-comparison-of-state-level-data-policies/.

Parsheera, Smriti. "Stack Is the New Black?: Evolution and Outcomes of the 'India-Stackification' Process." *Computer Law & Security Review* 52 (April 2024): 105947. https://web.archive.org/web/20240306042633/https://www.sciencedirect.com/science/article/abs/pii/S0267364924000141. https://doi.org/10.1016/j.clsr.2024.105947.

Paul, Surjit, and Saini Das. "Accessibility and Usability Analysis of Indian e-Government Websites." *Univers. Access Inf. Soc.* 19, no. 4 (2020): 949–57. https://web.archive.org/web/20240815122338/https://link.springer.com/article/10.1007/s10209-019-00704-8. https://doi.org/10.1007/s10209-019-00704-8.

Policy on Adoption of Open Source Software for Government of India, F. No. 1(3)/2014 – EG II (2014). https://www.meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf.

Policy on Collaborative Application Development by Opening the Source Code of Applications (2015). https://www.meity.gov.in/writereaddata/files/policy_government_application.pdf.

Policy on Open Application Programming Interfaces (APIs) for Government of India, Pub. L. Nos. F.No. 1(4)/2014-EG II (2015). https://www.meity.gov.in/writereaddata/files/Policy%20for%20API%20for%20GoI.pdf.

Policy on Open Standards for e-Governance (2010). https://egovstandards.gov.in/sites/default/files/2021-07/Policy%20on%20Open%20Standards%20for%20e-Governance.pdf.

Prakash, Pranesh, and Sajjad Anwar. "Two Experts Decode New Mapping Policy Guidelines, Explain Why This Is a Giant Leap Forward for India." *News18*, February 20, 2021. https://web.archive.org/web/20230829053902/https://www.news18.com/news/opinion/two-experts-decode-new-mapping-policy-guidelines-explain-why-this-is-a-giant-leap-forward-for-india-3454637.html. https://www.news18.com/news/opinion/two-experts-decode-new-mapping-policy-guidelines-explain-why-this-is-a-giant-leap-forward-for-india-3454637.html.

Press Information Bureau. "Summary of the Union Budget 2023-24." February 1, 2023. https://web.archive.org/web/20231115184526/https://pib.gov.in/Pressreleaseshare.aspx?PRID=1895320. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1895320.

Rajashekar, T.B. "Open-Access Initiatives in India." In *Open Access and the Public Domain in Digital Data and Information for Science: Proceedings of an International Symposium.* National Academies Press, 2004. https://web.archive.org/web/20230712073518/https://nap.nationalacademies.org/read/11030/chapter/35. https://doi.org/10.17226/11030.

Right to Information Act. Accessed July 16, 2023. https://www.media.gov.lk/images/pdf_word/2016/12-2016_E.pdf.

Roy, Raktima, and Gabriela Zanfir-Fortuna. "The Digital Personal Data Protection Act of India, Explained - Future of Privacy Forum." Blog. *Future of Privacy Forum*, August 15, 2023. https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/.

Singh, Vijaita. "Transfer of Personal Data Under U.N. Treaty Will Be According to Native Laws." India. *The Hindu*, September 13, 2023. https://web.archive.org/web/20231120073237/https://www.thehindu.com/news/national/transfer-of-personal-data-under-un-cybercrimes-treaty-will-be-in-accordance-with-domestic-laws/article67303701.ece. https://www.thehindu.com/news/national/transfer-of-personal-data-under-un-cybercrimes-treaty-will-be-in-accordance-with-domestic-laws/article67303701.ece.

Sorabjee, Soli J. "Introduction to Judicial Review in India." *Judicial Review* 4, no. 2 (1999): 126–29. https://web.archive.org/web/20231110074205/https://www.tandfonline.com/doi/abs/10.1080/10854681.1999.11427060. https://doi.org/10.1080/10854681.1999.11427060.

The Collection of Statistics Act, Act 7/2009 (2008). https://www.indiacode.nic.in/bitstream/123456789/2081/1/A2009_07.pdf.

The Hindu. "Data Protection Bill Poses Severe Restrictions to RTI Act, Advocacy Group NCPRI Cautions Government." India. July 14, 2023. https://www.thehindu.com/news/national/government-severely-restricting-rti-act-through-data-bill-ncpri/article67080300.ece.

The Wire. "'Regressive Amendments to RTI Act': NCPRI Flags Concerns Over Digital Personal Data Protection Bill." August 4, 2023. https://web.archive.org/web/20230820033005/https://thewire.in/rights/regressive-amendments-to-rti-act-ncpri-flags-concerns-over-digital-personal-data-protection-bill. https://thewire.in/rights/regressive-amendments-to-rti-act-ncpri-flags-concerns-over-digital-personal-data-protection-bill.

Vital Statistics Division. "Civil Registration System." Census of India, 2021. https://web.archive.org/web/20240630161120/https://censusindia.gov.in/census.website/node/180. https://censusindia.gov.in/census.website/node/180.

Wikipedia. "National Digital Library of India." June 27, 2024. https://en.wikipedia.org/w/index.php?title=National_Digital_Library_of_India&oldid=1231226458.

Wright, Glover, Pranesh Prakash, Sunil Abraham, and Nishant Shah. *Open Government Data Study: India*. Transparency and Accountability Initiative, 2010. https://cis-india.org/openness/publications/open-government.pdf.