KONRAD ADENAUER STIFTUNG

Data and Innovations: Through the Lenses of Health and Finance in India

Karthik Nachiappan, Natalie Pang and Kwang Lin Wong
National University of Singapore

DATA AND INNOVATION IN ASIA-PACIFIC

www.kas.de

CONTENT

PREFACE

Data fuels digital change. It forms the basis for numerous new products and services and can bring about specific advantages such as personalised medicine, autonomous driving, or more efficient administration. While data may be indispensable for the generation of new knowledge and may aid rational decision-making in the spheres of politics, society, and the economy, it brings with it an element of fear, stemming from issues such as vulnerable consumers, privacy concerns, and the possibility of algorithm-based decisions being executed independent of human control.

The ability to collect and process ever-increasing amounts of data is **key to innovation and growth**. For states such as Germany with a globally networked and high-tech economy, this presents enormous opportunities – especially due to the increasing amount of non-personal data made available through industrial processes as well as public sources. However, neither Germany nor Europe is fully exploiting the potential of data to drive innovation for the benefit of society, the economy, science, and the state. The collection and analysis of data does not have to be in conflict with the European approach to data protection, which sets an important standard for the responsible handling of data in the global context.

Numerous US and Chinese companies have occupied central and strategic positions in the global digital economy in recent years. These include cloud systems, digital payment systems, online trading, and Artificial Intelligence (AI). **Despite some notable successes, Europe and Germany still lack a comprehensive vision for the "age of data".** Nevertheless, in the spring of 2020, the European Commission launched its roadmap for digital policy – a "Data Act" to create a single European data market is planned for 2021.

Against this background, it is worth taking a **comparative look at the Asia-Pacific region** as it is generally considered the region that currently leads in both global innovation and economic growth.

Hence, the Konrad Adenauer Foundation's regional programme "Political Dialogue" based in Singapore started a large-scale study in September 2019 on data and innovation in the Asia-Pacific. We want to turn our gaze away from Silicon Valley to other important "data nations" in order to investigate the ambiguous and not-at-all-clear **connection between the use of digital data and the innovative capacity of economic and social systems**. However, we will not limit our analysis to technical and economic issues as the exploration of this ambiguous connection inevitably involves the fundamental political question concerning the systemic competition between liberal-democratic societies and authoritarian development models – in particular, that of the People's Republic of China – with regard to the manner in which data is obtained and used. To put it more pointedly, the question is: in times of omnipresent data generation and its use by increasingly AI-based systems, is the ability to innovate only to be had at the price of the complete disclosure of private data to governments and corporate actors? Or can an alternative approach, one balancing both the protection of basic rights and promotion of innovation, be found?

The study was carried out in collaboration with the National University of Singapore (NUS) and was supported by the country offices of the Konrad-Adenauer-Stiftung in the Asia-Pacific. We selected **Hong Kong SAR, India, Japan, the People's Republic of**

China, Singapore, South Korea, and Taiwan as the contexts to be examined. We looked at the areas of transport, finance, administration, health, and Industry 4.0 to understand how added-value for society and the economy can be cre-ated through modern data use.

We aim to contribute to the discussion on how to balance data usage and data protection in order to promote innovation in this digital age.

The following questions guided us in this study:

Narratives

How do companies, state actors, and civil society understand the handling of data – especially personal data – and the ethical assessment of such use? What are the prevailing narratives in each country?

Legal Bases

What are the laws and regulations that apply to the collection, use, storage, provision, disclosure, retention, and disposal of personal and non-personal data? What is the status of the development of legislation for these matters and how do different stakeholders deal with the issues of data protection and data portability between different (private and public) systems?

Ecosystem

Data is part of a larger "innovation ecosystem". Its potential can only be realised through interaction with other innovation-promoting elements. What specific legal, technological, infrastructural, cultural, and economic aspects of a country shape the respective ecosystems and determine performance?

This second report begins with a study on India, and focuses on the cases of FinTech and digital health. The report shows the range of efforts that the Indian government has invested in and contributed to in the FinTech and e-health spaces to spur innovation. FinTech adoption and development has been facilitated by the government's IndiaStack framework, which has generated a landscape wherein firms, businesses and citizens interact and transact digitally. Several digital health initiatives are currently afoot to transform the administration and delivery of healthcare. Advances in both areas, however, have occurred without a comprehensive data protection framework, which, once enacted, could complicate and constrain innovation.

We hope that the diverse pictures presented on the subject of data and innovation in Asia will provide food for thought in Germany, Europe, and Asia itself.

Dr. Peter Hefele
Director Asia and the Pacific

SUMMARY

This report shows the range of efforts that the Indian government has invested in and contributed to in the FinTech and e-health spaces to spur innovation.

Here are some key findings:

1. **India is the top market for FinTech investment in Asia and has the highest adoption rate of FinTech in the world.** India's FinTech trajectory has been shaped by regulatory and technological developments, coupled with business opportunities and gaps for domestic and foreign financial institutions and tech firms. Rising internet and mobile penetration since the late 1990s has boosted FinTech development, adoption and use.

2. FinTech innovation has been catalysed by the **indigenous technologies produced by the Indian state under the IndiaStack framework,** which has resulted in the emergence and use of interoperable public digital platforms through which Indian citizens transact. The Stack's backbone is Aadhaar, the biometric database that provides unique, verifiable identities to Indian citizens. These identities are used by FinTech firms to provide services to citizens following verification.

3. The FinTech transformation is designed to advance domestic development priorities including, most importantly, **financial inclusion** and access.

4. **Regulation** and governance of FinTech is **fragmented, broken across agencies** that regulate different aspects of digital finance, including finance, banks, IT, etc. Multiple rules and jurisdictions exist vis-à-vis data, which could stifle future FinTech innovation. Innovation requires a clear, transparent data governance architecture.

5. India's digital health landscape is diverse and broad, involving services, platforms, applications and softwares that seek to provide a digital analogue to existing health services.

6. Digitalisation in health is accelerated by the Indian government's plans to transform its domestic public health system in order to expand coverage and lower costs. **India's health ministry already uses several digital platforms through which it provides various services.**

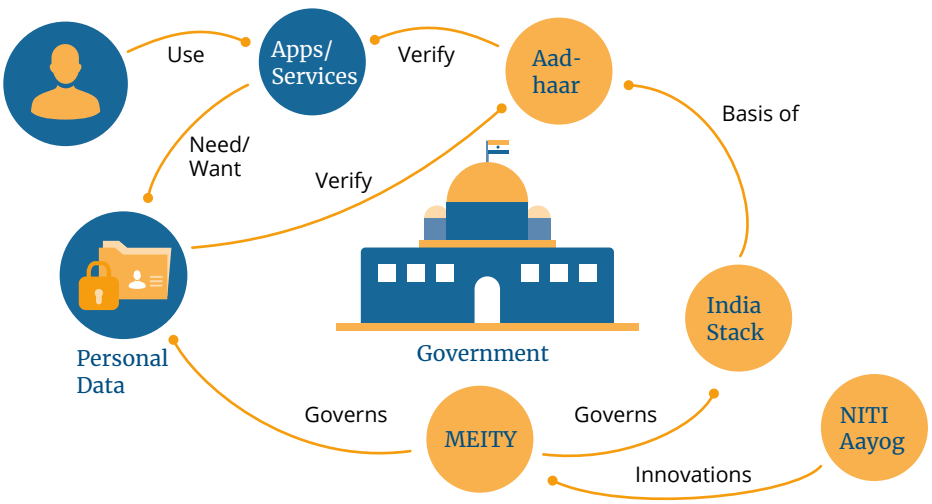
7. Digitising health information and data is a key component of transitioning to a more digital healthcare system. Plans are afoot to establish a **new digital health authority** that will govern digital health and be responsible for instituting new digital health standards and rules.

8. The establishment of new digital health initiatives and mechanisms are occurring **in the absence of a broad data protection framework** that could affect the processing, storage and sharing of sensitive health data.

INTRODUCTION

This project seeks to identify the features of data innovation in India, focusing on two specific domains – finance (FinTech) and health. It is the second in a series surveying seven different Asian territories to deepen understanding of innovation and data policies, and to contribute to debates which often focus on European models of data protection, such as the General Data Protection Regulation (GDPR). This report focuses on two policy areas where innovation has occurred in the absence of a comprehensive data protection law that could affect how governments, firms, organisations and individuals interact for personal and commercial purposes. **Through the key cases covered in this report – in the finance and health domains – we also consider and unpack how different actors operate and innovate in a policy vacuum.**

Policy innovations by the Indian government are currently spearheaded by the **National Institution for Transforming India (NITI Aayog)**. This agency operates as the in-house think tank that designs strategic and long-term policies and programmes for the government. One key function of NITI Aayog is to create an innovation-centred support system through a collaborative community of both national and international experts. The agency has also led initiatives related to e-governance and contributed to the conceptualisation of a tech stack or 'India Chain' that would create a nation-wide blockchain network through which government agencies can function. There exists a vision to connect India Chain to the existing **India Stack**, the digital infrastructure that powers Aadhaar, India's biometric identity database. Matters related to personal data and privacy are governed by the **Ministry of Electronics Information Technology (MEITY)** and the Information Technology Act (2000) which is administered by the ministry. Regulations pertaining to data are viewed not necessarily from an innovation lens but from the perspective of advancing the developmental aspirations and functions of the state. The state, thus, effectively conceptualises data as an asset that could unlock new pathways and trajectories of state action and power. As of now, the draft legislation governing personal data, the Personal Data Protection Bill (PDPB), put forth by the government appears to serve state and not citizens' interests. **Regulations in India are largely seen as stymieing and thwarting, rather than driving or fuelling innovation.**



> Regulations pertaining to data are viewed not necessarily from an innovation lens but from the perspective of advancing the developmental aspirations and functions of the state. The state, thus, effectively conceptualises data as an asset that could unlock new pathways and trajectories of state action and power.

India is the top market for FinTech investment in Asia and has the highest adoption rate of FinTech in the world (Invest India, 2020), and both local and multinational companies have launched FinTech services in the country. Developments in data governance in the Indian financial sector would thus have implications for the industry globally. As for health technology, with the Digital Information Security in Healthcare draft act released in 2018 and the National Digital Health Blueprint released in 2019, scrutiny regarding how health data should be treated accompanies expectations that the healthcare technology market will see significant growth in the near future.

This report will begin with an introduction to the Indian context and the key trends and organisations central to data governance, with a focus on the finance and health sectors. After that, it will delve further into issues concerning data and innovation in these sectors. Finally, the report concludes with an overview of the factors and considerations that drive innovation in India while looking ahead to how these perceptions around data might evolve in the future.

Innovation and Regulatory Landscape

To grasp the innovation and regulatory landscape in India, here's a list of the key stakeholders.

The **NITI Aayog** is a policy think tank of the government of India that was established to support the achievement of sustainable development goals by designing strategic and long-term policies for the government of India while providing technical assistance to central ministries and state governments.

The **Ministry of Electronics and Information Technology (MEITY)** oversees most policy issues under the remit of information technology, including e-governance, internet governance, needs and wants of the information technology sector, research and innovation promotion, fostering of human capital for the information and communications technology (ICT) transformation, development and management of digital services, and an open and safe cyberspace. MEITY also oversees the administration and regulation of the Information Technology Act, the chief legislation governing IT issues, including personal data.

The **Unique Identification Authority of India (UIDAI)** is a statutory authority and department established under MEITY to implement the Aadhaar programme, including owning and operating the Aadhaar database. Aadhaar provides digital identities for Indian citizens.

Under MEITY, the **National Informatics Centre (NIC)**, an agency established in 1976, has been responsible for mainstreaming information technologies into the delivery of government services to citizens. NIC is the chief promoter of digital opportunities for sustainable development and has led several initiatives that have implemented ICT applications in social and public administration. Through its flagship ICT network, NICNET, the agency has established institutional linkages with all other ministries and departments of the central government, state governments and districts across the country. NIC has also led government efforts to develop and incorporate innovative technologies in governance across all levels, including founding several "Centres of Excellence" for artificial intelligence and data analytics. NIC is also responsible for managing Computer Emergency Response Teams (CERT), which protect public infrastructures from cyber-attacks and threats.

The **Reserve Bank of India (RBI)** is India's central bank. It is responsible for the governance of financial technologies. The RBI sets the regulatory framework on financial technologies, responding to the dynamics of the rapidly evolving FinTech landscape. The RBI also introduced a framework for a regulatory sandbox where the financial sector regulator provides new guidances and rules to facilitate interactions between specific jurisdictions, in order to increase efficiency, manage risks and create new opportunities for consumers.

The **National Payments Corporation of India (NPCI)** operates all retail payment and settlement systems in India. It was established as a non-profit organisation by the RBI in 2008 and is now owned by a consortium of major Indian banks. The organisation manages both RuPay, a robust card system that enables banks and financial institutions to implement electronic payments, and **Unified Payments Interface (UPI)**, a system that allows customers to initiate and complete payments through mobile devices.

The **Ministry of Health and Family Welfare (MOHFW)** oversees health and family planning policy in India. The ministry published a draft of the **Digital Information Security in Healthcare Act (DISHA)** in 2018 to regulate the creation, collection, storage and sharing of health data. It also proposed the establishment of a National Electronic Health Authority charged with creating guidelines and standards for digital health data.

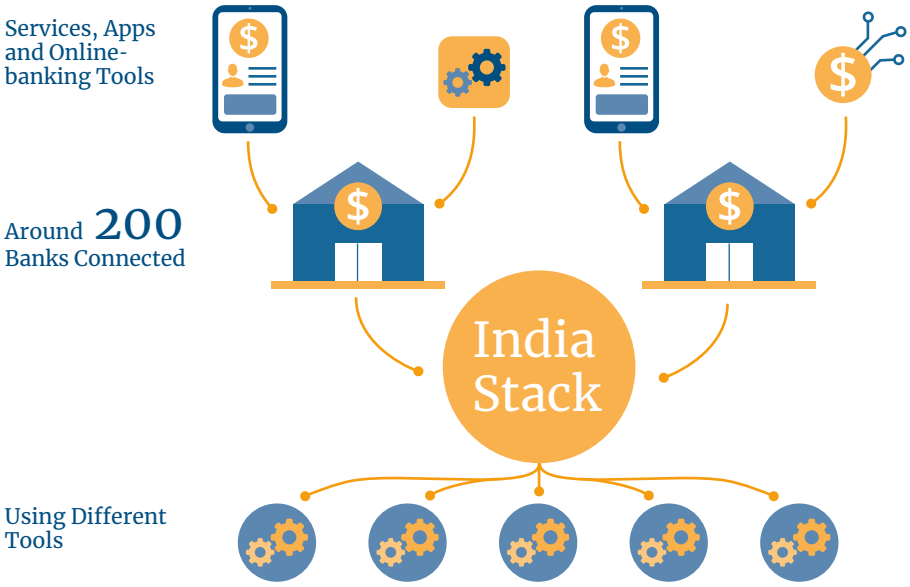
Case 1

India's FinTech

Landscape and Activities

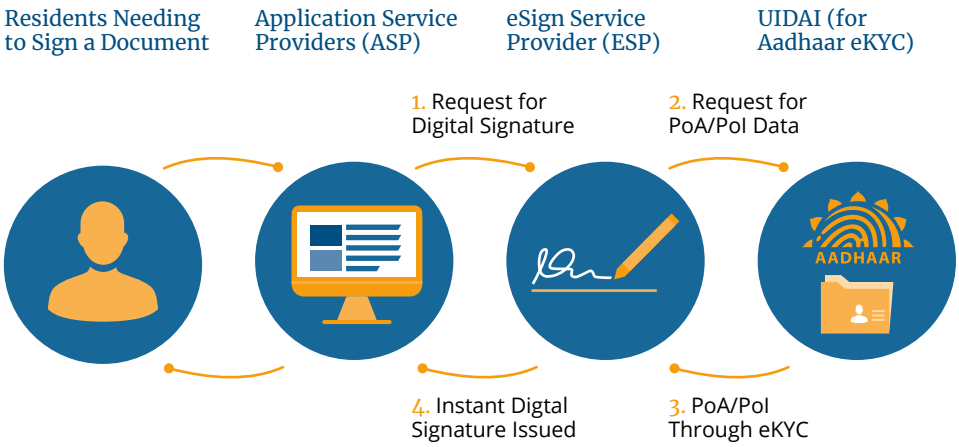
India's FinTech industry is the product of several drivers, technological and regulatory, coupled with an increasing number of business opportunities and gaps that are somewhat specific to India. The domestic FinTech revolution sits on the tremendous strides made in internet and mobile penetration since the late 1990s. According to the Department of Telecommunications (DOT), India has nearly 1 billion wireless subscribers in March 2020 (TRAI, 2020). Per capita internet use has been increasing, and so has wireless data usage. Demographics have boosted India's FinTech trajectory. Besides these structural features, India's FinTech revolution has been fundamentally led by the India Stack framework, a range of indigenous technologies that has catalysed innovation in this space (D'Silva et al, 2019). The India Stack framework has involved the development of secure, interoperable digital platforms that serve as public goods for Indian citizens and firms (D'Silva et al, 2019). **The Stack's backbone is Aadhaar, the biometric database that provides unique, verifiable identities to Indian citizens. These identities can then be used by FinTech firms to provide services to citizens following verification (UIDAI, 2019).** Through Aadhaar, other public digital platforms have been developed, including e-KYC, which verifies customers; e-sign for digital signatures; DigiLocker, which provides cloud storage; and other payment-related services that facilitate financial interactions between service providers and customers.

> The India Stack framework has involved the development of secure, interoperable digital platforms that serve as public goods for Indian citizens and firms.



For payments, the United Payments Interface (UPI) serves as a crucial accelerant, allowing customers to use the virtual interface to transact with one another digitally (RBI, 2018a). As of now, 200 Indian banks operate on the UPI system, through which FinTechs gain access to all existing consumer and business bank accounts to facilitate payments. Banks need not interact or establish distinct relationships with one another to access each other's customers and their bank accounts. With this function sorted out, payment and FinTech apps focused their time on acquiring customers, bettering their products, and making them more accessible and amenable for public use, rather than on how to fashion workable relationships between themselves to facilitate financial transfers (Vir & Rahul, 2020).

As of now, 200 Indian banks operate on the UPI system, through which FinTechs gain access to all existing consumer and business bank accounts to facilitate payments.



Several definitions of FinTech exist. It is regarded as **'technology-enabled' financial solutions that could include and go beyond products and services banks traditionally provide**. Another definition identifies FinTech as an 'economic industry composed of companies that use technology to make financial systems more efficient' (D'Silva et al, 2019). The Basel Committee on Banking Supervision (BCBS) defines FinTech as 'technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and their provision of financial services' (Basel Committee on Banking Supervision, 2018). The Basel definition incorporates business models, processes, and products into its FinTech conception; essentially, this definition pegs FinTech to the financial sector and considers FinTech as a function of finance related to how countries organise their financial industry and deploy it to fulfil outcomes. It is appropriate to use the Basel definition to classify FinTech in India, given the emergent FinTech sectors' close links with the mainstream financial sector and their material effects on the industry.

FinTech firms are increasingly enablers, drivers of an unprecedented transformation in how Indian citizens accumulate and deploy finance for different purposes.

FinTech in India refers to technologically intensive financial applications, platforms, products, and services developed for a domestic market that demands innovative solutions to meet their financial needs, including payments, deposits and lending, wealth and investment management, capital markets, and insurance. Generally, FinTech firms and applications are no longer seen by banks and other financial institutions as disruptive entities. They are increasingly enablers, drivers of an unprecedented transformation of how Indian citizens accumulate and deploy finance for different purposes. As a result, banks are collaborating with FinTech services and firms to provide a range of different tools. Collaboration involves investing in FinTech firms, launching subsidiaries, and transferring certain operational functions. Synergies exist. FinTech firms, given their generally nimble size and portfolios, lack what banks have – a large client pool and regulatory knowledge, having already navigated the labyrinth that is the Indian financial sector.

FinTech firms also piggyback on the trust and reputation these banks have built over decades. Trust comes in handy when FinTech firms require support managing and meeting specific regulations and rules. For banks, FinTech firms offer and present opportunities to extend their businesses into areas hitherto untapped and to reach both new and unbanked customers. Through various FinTech partnerships, banks can diversify into and enter areas like insurance, brokerage, asset management, and related services to generate greater revenues and profits.

Going by this definition, we can map several different FinTech-focused activities in India. The hallmark of India's FinTech landscape is diversity when considering markets, services, and applications.

- **Payments:** Most FinTech-oriented or -related applications focus on payments that are highly regulated in India. Applications covering payments perform basic functions that include conducting digital payment transactions, providing payments services or acting as payment gateways, aggregating and executing payments, etc. FinTech applications covering payments use the channels developed by the National Payments Corporation of India (NPCI). Most payment apps use either the Immediate Payment Service (IMPS) or the Unique Payment Interface (UPI) managed by the NPCI. However, applications that use the NPCI base must possess a license from the Reserve Bank of India to provide mobile banking services. Another aspect of digital payments involves payment gateways governed by industry standards – Payments Card Industry Data Security Standards (PCIDSS). Most payment-oriented digital solutions create products like Paytm and Google Tez that use the underlying UPI or IMPS infrastructure. Payment gateways ensure transactions are completed and verified securely.

- **Deposits:** Several Peer-2-Peer lending platforms exist in India that provide loans to consumers and businesses once documentation is verified to ensure creditworthiness.

- **Investment and wealth management:** Digital applications and services allow consumers to track wealth portfolios, expenses, and inflows of income and related capital.

- **Insurance:** Some financial institutions provide insurance options through intermediaries for consumers. Certain firms also use data from devices and mobile devices to verify claims and finalise personalised premiums for insurance products.

India's FinTech revolution is designed to address domestic exigencies.

1. **The FinTech trajectory helps Indian users transact with one other and with banks and other financial intermediaries through FinTech apps and services. The prevailing focus is to enhance and facilitate payments within Indian borders, not beyond.** To be sure, cross-border payments do take place, but they are not an essential priority. Cross-border financial transactions lag behind domestic payments, and the landscape is overwhelmingly tilted to service the latter, not the former. However, scope exists to make India's unique payments system compatible with that of other jurisdictions, provided the latter can also fulfil regulations and follow procedures that the Indian Stack has established, like Know Your Customer (KYC) and Anti-Money Laundering (AML).

2. **As a result of this domestic impetus, momentum has been generated around a data governance architecture that favours localisation or domestic retention and data processing.** The fallow nature of cross-border payment flows also means that pressures to allow for more data sharing are not present or serious. As India

becomes 'data-rich', the focus will be on establishing and passing domestic rules that protect data whilst making that data available to agencies, regulators, consumers, and firms to leverage on for private and public gain. Pressures will gather around empowering citizens and consumers through the data generated.

As India becomes 'data-rich', the focus will be on establishing and passing domestic rules that protect data whilst making that data available to agencies, regulators, consumers, and firms to leverage on for private and public gain.

3. FinTech developments seek to expand financial access and inclusion through high mobile and internet penetration. **Despite record strides being made, more efforts are needed to redress inequality when it comes to FinTech access.** Digital ecosystems and marketplaces have to be rendered more trustworthy to draw untapped users.

4. **FinTech applications and tools seek to expand financial access to debt and equity, even for those lacking a sufficient capital base from which they can draw.** This approach provides new customers with more options should they find difficulties obtaining financing through mainstream lending channels and standards.

Stakeholders and Relationships

Policies that affect innovation and experimentation in India's financial industry, which has rapidly digitised over the past decade, are undertaken by different agencies. Over the span of just a decade, India has gone from being a largely cash-based economy to one heavily reliant on digital payments. **This spectacular transition has been facilitated by domestic programmes like Aadhaar, Unified Payments Interface (UPI), India Stack and a litany of digital wallets developed by private companies, such as Mobikwik, PayTM and PhonePe.** International firms have also entered the digital payments market in India, with Google Pay, Amazon Pay and WhatsApp Payments rolling out their services in the country.

Over the span of just a decade, India has gone from being a largely cash-based economy to one heavily reliant on digital payments.

Both the IT Act and the NSCP have been bolstered by the formulation of specific technical rules and standards from related government departments and agencies that focus on issues like data protection, mobile banking and encryption.

The chief FinTech regulator is the Reserve Bank of India (RBI), which has, thus far, opted to manage the sector with a light hand (Reserve Bank of India, 2016)**.** As of now, there are very few regulations or policy guidelines governing FinTech, though the central bank has regularly released policy notes and advisories for domestic banks and other payment operators. The RBI has chosen to take the lead from market developments and technological advancements when crafting rules. Rules are simpler for existing financial institutions that are developing new applications for customers to make

payments; new non-bank or financial institution operators must follow certain rules vis-à-vis compliance and customer identification before operating as a FinTech service.

As the volume and intensity of digital financial transactions have grown, the RBI has moved to ensure sufficient mechanisms exist to avoid unauthorised or deficient behaviours. In 2017, the RBI issued guidelines for India's growing system of digital wallet operators to ensure transaction authentication and fraud prevention (as of March 2019, 58 digital wallet operators exist in India) (Patil & Chakraborty, 2019). The bank has also ensured that Indian customers have sufficient protections should they become exposed to fraud, negligence or related breaches within the expanding digital payments ecosystem. Some of these rules are similar to regulations governing retail banking. India has always had a heavily regulated banking sector that has erred on the side of safety and caution, not experimentation and innovation.

In terms of data, the RBI has mandated the storage of domestic payment data in India, for security reasons as well as in recognition of the difficulties associated with obtaining payment data stored abroad despite the existence of several Mutual Legal Assistance Treaties (MLATs). Given the rising number of cyber attacks and crimes, the RBI has mandated banks to establish security operations centres (SOC) to detect and report cybersecurity incidents (Reserve Bank of India, 2018b). SOCs are expected to report these threats and incidents to the Indian Banks-Center for Analysis of Risks and Threats (IB-CART), a repository where cyber threat information will be collated (Reserve Bank of India, 2016). To enhance cybersecurity for digital payments, the Indian government has plans to create several more specialised cyber agencies, including a new Indian Cyber Crime Coordination Centre and Computer Emergency Response Teams for the Financial Sector (CERT-FIN) (Department of Economic Affairs, Ministry of Finance, 2017).

The push toward digital payment systems was accelerated by the Indian government's Aadhaar programme, the world's largest biometric identity project. Aadhaar provides every Indian citizen with a verifiable electronic identity, thereby facilitating their entry into the mainstream financial system. **With access to the Aadhaar digital identity system, financial institutions were able to access and onboard customers at a much lower cost and with greater efficiency, since Aadhaar facilitated biometric authentication and digital access.** Remote digital access would have been particularly significant in increasing accessibility for the urban poor and rural segments of the market (Bhakta, 2018). The UIDAI manages and administers the Aadhaar programme, setting the framework that allows FinTech institutions to draw in citizens and make them digital customers (Ahluwalia, 2020).

The push toward digital payment systems was accelerated by the Indian government's Aadhaar programme, the world's largest biometric identity project. Aadhaar provides every Indian citizen with a verifiable electronic identity, thereby facilitating their entry into the mainstream financial system.

However, a September 2018 court ruling rescinded the right of private entities to access the Aadhaar biometric database even with the individual's consent, so as to keep biometric data and each person's unique identification number confidential. While alternative models have been proposed, such as using the QR codes on Aadhaar cards for authorisation, these would entail more costs and a lengthier process that may discourage both clients and financial institutions from using Aadhaar at all. Furthermore, ambiguities remain to be clarified regarding the exceptional conditions under which Aadhaar authentication would be permitted for banks and non-banking financial institutions. For example, in October 2018, the UIDAI announced specific conditions under which banks could use Aadhaar cards for authentication or to open bank accounts, but it remains unclear if these rules apply to financial institutions without a bank license. Furthermore, RBI regulations have not been amended to recognise these exceptions.

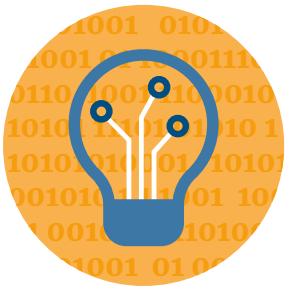
As FinTech broadly refers to services and products that cut across both technology and finance, ranging from traditional banking to new areas like blockchain, artificial intelligence, cybersecurity, data, cloud computing and cryptocurrency, this overlap has also shaped how the Indian government has approached the sector in terms of managing it (Reserve Bank of India, 2019).[1] **Regulation and governance are fragmented.** Several regulators exist. Stakeholders range across Indian state agencies and beyond them. FinTech has also become critical to India's development, given transformative developments in public infrastructure with the rise of critical initiatives like Aadhaar and the United Payments Interface (UPI) (Gupta, 2018).[2] Collaboration is thus required to ensure regulation does not trample innovation.

1 Reserve Bank of India, 'Report of the High Level Committee on Deepening of Digital Payments', May 2019 (https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CDDP03062019634B0EEF3F7144C3B65360B280E420AC. PDF).

2 Gupta, K. (2018). 'UPI 2.0 launched. Here are its key features,' Livemint. (https://www.livemint.com/Money/Cog3dAvOZka0OsNg8M9S8O/UPI-20-launched-Here-are-its-key-features.html).

India's federal structure affects policies and regulations covering FinTech. **Cross-cutting jurisdictions and the rising number of agencies that have authority over finance and technology have constrained the establishment of consistent rules.** Most regulations covering the banking and financial sector are drafted and passed at the level of the central government while being implemented by states. For instance, the Payment and Settlement Systems Act 2007 and 2018, which provides for the authorisation, regulation and supervision of the RBI's payment systems, was nationally drafted (National Payments Corporation of India, 2018).[3] Recent amendments to the Act (2018) have focused on updating provisions as digital payments proliferate. Certain states have also drafted specific FinTech policies. Maharashtra, where the financial industry is based, has drafted a FinTech policy that focuses on establishing regulatory sandboxes and advancing FinTech start-ups (Singhal, 2019).[4]

That said, financial innovation in India is constrained by competing jurisdictions that govern technology and digital issues. Laws are yet to be enacted on several critical technology-related issues, including data protection, artificial intelligence, cybersecurity, cloud computing, etc. **Existing laws like the Information Technology Act (2000), which has provisions covering some issues like data and cybersecurity, particularly cybercrime, are largely ill-equipped to deal with the challenges posed by digitalisation in 2020.** The lack of statutory clarity will likely affect how firms and start-ups in the Indian financial sector operate; indeed, new laws could complicate innovation, if not bury it, since existing laws already present challenges in clarity and coordination across different forms of data processing and institutions. **The existence of multiple regulations across jurisdictions will likely induce policy uncertainty.**



Data Cultures

Debates around data privacy are currently being held in parliament through the 2019 Personal Data Protection Bill. For legal experts, privacy activists, industry groups and entrepreneurs, the Indian government appears set to sacrifice privacy at the altar of controlling the reams of data being generated and harvested and leveraging it for public use. **Despite a recently enshrined constitutional right to privacy, there's a sense from some of the interviewees that existing laws governing privacy and the prospective one will serve to stifle digital innovation and e-commerce.** For instance, one interviewee, an expert working on political economy issues within India, alluded to the disruptions that companies might face when complying with the new regulation – big tech companies will have to resolve the friction between the Indian regulation and foreign regulations, while smaller domestic companies will have to rebuild their protocols and alter their business models to ensure that they comply with the new laws. Since big companies that already have ample resources would be better able to adapt to new regulations, this may have the effect of stifling competition in the market, at least in the short term. There is also the possibility that the new laws will harm the existing protections citizens and users of different applications possess currently. For example, another interviewee foresees a

3 NPCI, 'Retail payments statistics on NPCI platforms' (https://www.npci.org.in/sites/default/files/RETAIL%20PAYMENTS%20STATISTICS%20ON%20NPCI%20PLATFORMS%20-%20June%202018_1.pdf), accessed 11 August 2020.

4 Singhal, Aastha. 2020. 'Mumbai Thrives to Become the FinTech Hub". Accessed 4 October 2020. (https://www.entrepreneur.com/article/333951).

misuse of powers by regulators to harass companies that are not "friendly to Indian interests or the government interests". It is also up to the regulators to decide if they would want to disclose whether an individual's data has been breached.

The first data protection legislation (2018) had robust safeguards that have been revised in the latest iteration of the bill – revisions that could make it antithetical to privacy, innovation and ensuring basic protections exist as citizens engage online. It appears as though the government will have the authority to access and use private and public data on the grounds of development and sovereignty; this will undermine both the right to privacy and data protection. Surprisingly, while there could be grounds to use data to develop better public policies, most of the experts conveyed their displeasure and anxiety, rather than sanguinity, with the deployment of data to provide public goods. These 'statist' data perceptions are heightened by recent developments with respect to non-personal or anonymised data. Increased government involvement in non-personal data could lead to a data governance terrain where the state dominates, possibly leading to anti-competitive tendencies across industries. The regulation of data, both personal and non-personal or anonymised, could engender a larger, more dominant state that engages with actors closely across markets or creates digital infrastructures under which other private actors operate.

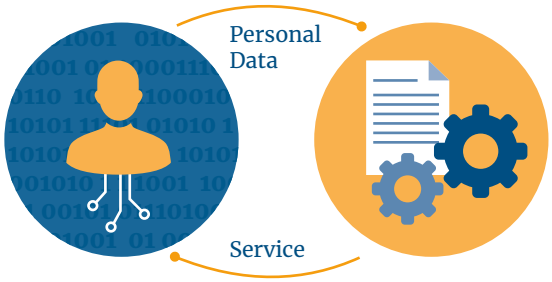
The FinTech sector is heavily regulated in India given the government's penchant for over-regulating the financial industry. **Unlike in other sectors, rules governing data exist, having been issued by the Reserve Bank of India, which mandates a copy of all payments data to be stored in India.** This requirement is referred to as **data localisation or data nationalisation**. With new legislation governing data, interviewees generally held that innovation will likely suffer and that the potential for the Indian FinTech scene to share data and collaborate with other jurisdictions will flag once new rules are enforced, sandboxes notwithstanding. If you break down the financial sector further, it is evident that the new legislation will likely have a greater detrimental impact on small and medium-sized firms when compared to larger firms who already comply with a broad swathe of regulations. Some of these smaller firms are also engaged in cutting-edge business analytics work that requires a lot of data; hence, the emphasis on localisation, partial or full, alongside additional regulations, jeopardises their existence, given the internal infrastructures they will have to establish to manage data-related queries and enquiries.

Some FinTech firms are also in the booming e-commerce domain, which requires fungible data-sharing rules. That said, most firms in India's booming FinTech sector will have to simultaneously comply with both domestic and foreign regulations with respect to privacy and data sharing; this will affect how such firms function and operate. Innovation could suffer from additional compliance burdens. Small and medium-sized financial institutions will have to bear additional costs vis-à-vis compliance that could affect their market operations and positions. This new regulatory burden will also be shared widely in the financial industry – firms, suppliers, vendors, intermediaries and those they transact with across sectors like education or healthcare – so the effects will be similar until they are borne by all parties. Firms in the financial industry will have to comply with new data laws that prioritise privacy, consent and accountability but flexibility will exist as to when and how they comply. Given the existence of regulators and rules that deal with data and privacy in the financial sector, most firms will likely continue to follow current rules until regulations have to be complied with. Some experts expect this lag to last until the new data protection law (2019) has sufficient writ and enforceability.

> Most firms in India's booming FinTech sector will have to simultaneously comply with both domestic and foreign regulations with respect to privacy and data sharing; this will affect how such firms function and operate.

Another interesting aspect of the emergent FinTech data culture is its increasing consent-oriented nature. Personal information is and will be procured from users only after extensive consent is provided; this could complicate the administration and enforcement of new data protection laws and make the 'downstream' aspects that involve the user or consumer onerous. **The consent-based approach in India's legislation was drawn from the EU's GDPR.** But is this consent-driven requirement domestically relevant? Given the weak understanding of consent rules and requirements amongst the Indian population, a rigid consent-oriented data protection regime might not be applicable for India. Nevertheless, firms will have little choice but to adhere to it given the requirements posed by foreign jurisdictions like the European Union. Some interviewees pointed out that Indian citizens have a transactional relationship with data, which suggests that they are mostly willing to disclose personal data as long as they receive a service or benefits in return. This implies that the current consent requirements may not be domestically urgent. **Indian consumers could find themselves dealing with a partly imported data governance environment that does not fit their specific needs or wants. At the same time, there will be increasing regulatory burdens for firms and organisations that have to institute stronger policies that protect personal data.** The tensions are clear. Industries like FinTech will have to balance the demands and obligations of starkly different domestic and foreign markets. That Indian FinTech firms have interests across the globe complicates their domestic positions and operations. Frictions will arise with competing data protection laws abroad. Should these laws not facilitate or lead to interoperable data-sharing pathways, firms will have to bear the responsibilities of managing their clients' data. A fragmented global data landscape will only serve to limit the potential of firms in different sectors, including FinTech, to innovate and develop products and services for the Indian market.

> Indian citizens have a transactional relationship with data, which suggests that they are mostly willing to disclose personal data as long as they receive a service or benefits in return.



Laws and Regulations

As of now, India does not have a data protection legislation. The existing framework that governs personal data is the Information Technology Act (2000) ("I. T. Act"), which contains, under Section 43A, rules regarding security practices and procedures when handling personal information (The Information Technology Act, 2000). The I. T. Act was amended in 2008 with the addition of subordinate legislation that deals with data, otherwise known as the Reasonable Security Practices and Procedures Rules (RSPP), which protect sensitive personal data (The Information Technology Act, 2000). The law itself does not proactively enforce rules regarding data collection and protection but instead allows citizens to claim compensation, should companies breach RSPP rules. Section 72 and 72A of the I. T. Act mandates criminal punishment should a government official or service provider disclose personal information without personal consent or if done to cause harm or wrongful loss (The Information Technology Act, 2000). Other privacy rules issued by the government have been piecemeal, and only apply should the RSPP not be viable.

> As of now, India does not have a data protection legislation.

Questions, however, have long existed regarding the RSPP's legal validity since there is no independent legal statute that compels organisations and firms to protect personal data. It is increasingly evident that the I. T. Act has also not been sufficiently enforced – this has precipitated other regulators to draft their own rules to manage gaps in data processing and storage. Like the financial industry, other sectors have not relied on the RSPP but have chosen to draft sectoral rules to govern data. The Reserve Bank of India (RBI) has issued circulars and notifications that oblige banks and other financial institutions to safeguard customer data. That said, it is essential to remember that banks in India have always been heavily regulated. Some of the new rules that banks have had to adhere to concerning cybersecurity emanate more from a desire to manage them closely than from specific concerns with data protection. Other regulatory agencies like Telecom and Regulatory Authority of India (TRAI) and the Security and Exchange Board of India (SEBI) have rules governing data in their remits though current data standards do not adequately protect telecom users and subscribers (Matthan, Venkataraman and Patri, 2017). New Delhi also relies on two additional tools that track personal information flows – the Central Monitoring System (CMS), which provides government officials with instant access to internet traffic flowing through specific networks, and the Networks Traffic Analysis (NETRA), which analyses internet traffic through terms like 'kill' or 'bomb'. Both have crystallised calls for a clear set of rules concerning privacy (Xynou, 2014). These tools, which essentially allow the central government to mass-monitor all telecommunications on phone networks and the internet, were developed in the name of national security, especially after the Mumbai bombings of 2008. However, a High Court ruling at the end of 2020 directed the central government to cease data collection through these systems as they constitute a breach of citizens' right to privacy (Gill, 2020).

Since 2017, Indian officials have been working to draft and enact a comprehensive data protection framework that codifies the recently enshrined right to privacy. Progress has been slow. The first draft legislation, released in 2018, sought to create a framework that sequestered data in India through provisions that called for 'data localisation' (Kalra, 2018). Citizens who were providing personal data were regarded as 'data principals' who held considerable rights that had to be respected and protected by 'data fiduciaries', organisations collecting personal data. These data 'fiduciaries' were accountable to the data 'principals'. Data sharing between and across jurisdictions was discounted given the government's desire to optimise data for policy purposes and to eschew relying on foreign jurisdictions for domestic data. Consent was integral to the collection and processing of data. Some of these provisions were revised in the second version of the legislation released by MEITY in December 2019. The bill is now being discussed within a Joint Parliamentary Committee before heading for a vote in the lower house of India's parliament.

Case 2

Digital Health

Mobile Health

Remote Diagnosis

Telemedicine

Landscape and Activities

Digital health (e-health) refers to computing services, platforms, applications, and software that deliver healthcare. These technologies generally have a wide range of uses, from mobile medical applications and software to creating and updating medical devices and products that help physicians and medical professionals make optimal clinical decisions (U. S. Food and Drug Administration, 2020). Broadly, however, these uses revolve around one driving motivation – to accurately diagnose and treat various health conditions and diseases. Such tools offer great opportunities for better medical outcomes across the board by deploying various technologies and applications.

Using this definition, we can identify several activities that fall under India's rubric of digital health.

- **Mobile health:** the use of mobile applications to connect physicians to patients to conduct remote consultations.
- **Remote diagnosis:** digital and portable tools that provide basic diagnostics and e-prescriptions, particularly useful for rural populations that live in remote areas.
- **Telemedicine:** refers to the use of technologies for remote diagnosis and monitoring across large areas, not just rural. Top hospitals also have integrated telemedicine centres and the capabilities to expand the range and scope of care provided.

- **Digital social health:** use of social media and social infrastructures as knowledge portals through which medical professionals share knowledge with users seeking help.
- **Wearables:** technologies that users can wear to track their diet and fitness activities and to measure basic health parameters like sugar level and heart rate.
- **Electronic medical records (EMRs):** EMRs are developed for healthcare providers to manage their healthcare operations, specifically patient records and data. Digitisation allows health providers to use I. T. systems and cloud computing to increase remote and immediate access to patient data.

Digital Social Health

Wearables

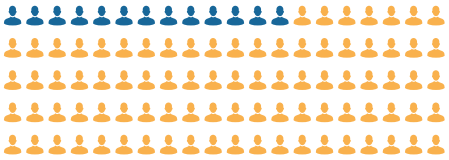
Electronic Medical Records (EMRs)

World's Largest Public Health Insurance Programme Aims to Cover 500,000,000 People

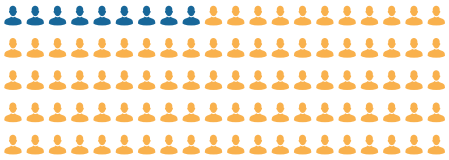
India appears to be on the cusp of transforming its domestic health system, with digital tools driving that shift. The Indian government recently launched the world's largest public health insurance programme, 'Ayushman Bharat'. This aims to cover 500 million people, who will likely receive care on digital platforms (Angell et al., 2019). The government has also been developing a new digital health strategy that will revolutionise how healthcare is provided in India. This strategy will supersede the digital health initiatives currently underway. The Future Health Index's 2019 report claims that India leads the world in the adoption of digital health technologies, with around 88% of healthcare professionals using and relying on digital health tools in their practice (Future Health Index, 2019).

> The Future Health Index's 2019 report claims that India leads the world in the adoption of digital health technologies, with around 88% of healthcare professionals using and relying on digital health tools in their practice.

A key function of digital health in India is to streamline the existing health apparatus by digitising it. Transitioning to digital health records and processes allows healthcare providers and physicians to improve their service delivery by creating accurate health records, keeping them updated, and enabling their transmission across the healthcare system to other providers who might require them to address a patient's condition. This process is being slowly implemented: **There has been a move to digitise medical records and data as part of the government's 2015 Digital India campaign, which seeks to deliver public services electronically.** Digital health technologies are a pivotal way to realise this objective – the delivery of efficient care across the healthcare system. India's healthcare system is highly heterogeneous; interactions between different layers and providers are uncommon, making cutting across these layers through technologies vital and necessary. Finally, tools like telehealth and telemedicine also help lower barriers for Indian citizens to access healthcare, thus increasing healthcare access and patient satisfaction. In 2019, 13% of Indian citizens in rural areas had access to a primary health centre and 9% to a hospital (PricewaterhouseCoopers, 2019). Digital health systems could enhance these individuals' reach, ensuring the delivery of preventive, curative, and other health services to address various health conditions.



13% Access to a Primary Health Centre



9% Access to a Hospital

Stakeholders and Relationships

In India, the **Ministry of Health and Family Welfare (MOHFW)** is responsible for the provision and delivery of public health. Under this broad remit, the MOHFW's E-Health and Telemedicine initiative manages and implements policies and programmes that use information and communication technologies to improve the efficiency and effectiveness of India's public health system (Ministry of Health and Family Welfare, 2020). Through digital tools and applications, the MOHFW seeks to address longstanding problems plaguing healthcare, including shortage of trained health professionals, inaccessible health infrastructures and unaffordable healthcare services. This initiative includes a wide range of programmes, including:

Wide Range of Programs

- National Health Portal (NHP)
- e-Hospital@NIC
- Online Registration System (ORS)
- Central Drugs Standards Control Organization (SUGAM)
- Food Safety and Standards Authority of India (FSSAI)

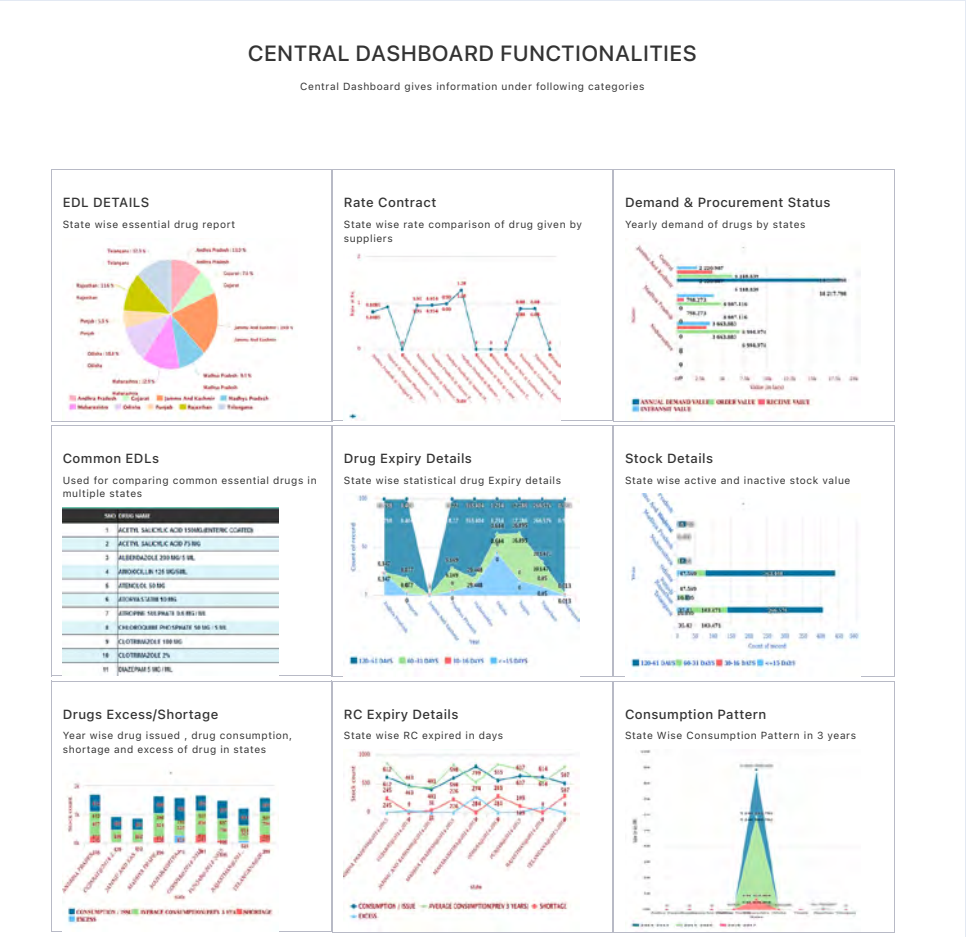
Various Mobile Applications

- Vaccine Tracker
- India Fights Dengue
- NHP Swasth Bharat
- No More Tension
- Kilkari
- Mera Aspataal (Ministry of Health and Family Welfare, 2019)

These MOHFW applications cater to various health and medical needs: checking dengue symptoms; general information on common diseases; stress management; reminders and tips on pregnancy and childcare; and collecting patient feedback on services at healthcare facilities.

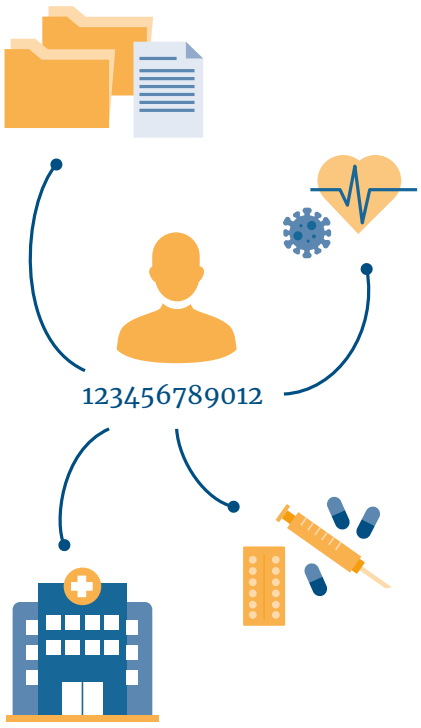
The MOHFW manages several digital service delivery tracking systems, like the Mother and Child Tracking System (MCTS), TB Patient Monitoring System, Tobacco Cessation Programme and mDiabetes programme. These services help citizens obtain more information about government health services. The ministry also runs some of its core functions through automated systems, including the Hospital Information (System), Drugs and Vaccines Distribution Management System (DVDMS), Health Management Information System (HMIS), Integrated Disease Surveillance Programme (IDSP) and the Central Dashboard. **The Central Dashboard, another MOHFW initiative, compiles data from public health information systems across states and ministry programmes (such as MCTS, IDSP and HMIS) in order to monitor key indicators on health programmes and track the progress of health initiatives. The Central Dashboard is primarily used by senior MOHFW officials for policy formulation and by state officials for monitoring and improving their policy measures.** Finally, the MOHFW manages the Indian government's global agenda on digital health. India is a founding member of the Global Digital Health Partnership, a collaboration of governments, territories, government agencies and the World Health

Organisation (Biospectrum Asia, 2019). The GDHP provides an international forum to facilitate global collaboration and share best practices and experiences on the implementation of digital health services. In 2019, India hosted the 4th GDHP Summit, where all signatories adopted the Delhi Declaration on Digital Health for Sustainable Development.



The Central Dashboard compiles data from public health information systems across states and ministry programmes in order to monitor key indicators on health programmes and track the progress of health initiatives.

Recently, the MOHFW called for the **establishment of a National Digital Health Authority (NDHA) to serve as the nodal agency for the formulation, adoption and regulation of eHealth standards across India** (Sarbadhikari, 2019). The NDHA will also act as the nodal agency for all strategic e-Health initiatives. To improve public health accessibility, the MOHFW has created a robust telemedicine infrastructure that facilitates the outreach of healthcare services to remote areas (Ministry of Health and Family Welfare, 2019a). **These telemedicine solutions are being provided to deliver basic and specialised healthcare services to those areas that lack health systems.** These telemedicine initiatives include National Medical College Network, National Telemedicine Network and the Use of Space Technology for Telemedicine. **Recently, the Indian government also announced the creation of National Digital Health Mission (NDHM), which will create unique health IDs to hold the digital health records of Indian citizens** (Singh and Porecha, 2020). The mission hopes to digitise the Indian health system, including how citizens engage and access different services, such as making doctor's appointments, depositing money, managing and securing health records, scheduling procedures, etc (Ministry of Health and Family Welfare, 2019b). As of February 2021, around 600,000 digital health IDs have been created by the government (Tandon, 2021). A pan-India health registry will maintain records that should be portable and accessible to all healthcare stakeholders, creating a system that would make electronic health records interoperable. **Tied to the health ID, these records will contain the entire health profile of Indian citizens, including details of illnesses, treatments, hospital stays and discharges alongside any tests or procedures they may have taken.** Digitisation could result in the streamlining of health services. This could in turn reduce health costs, which matter to the government, particularly with the introduction of the world's largest health insurance scheme, Ayushman Bharat, in January 2018 (Pareek, 2018). It is not clear whether the government will make these health IDs mandatory. Some of these digital health measures were part of the government's National Health Policy 2017, which envisaged the deployment of digital tools to improve healthcare provision in India (Ministry of Health and Family Welfare, 2019b). In addition, ensuring the security of the health data is a top priority, and various private sector actors have expressed their concerns and desire for a robust cyber-security infrastructure that goes beyond just designating consent managers (Khushhal, 2020).



India's National Health Policy 2017 calls for creating a digital health technology ecosystem that serves the needs of all stakeholders and improves efficiency, transparency and how citizens receive public and private healthcare (Ministry of Health and Family Welfare, 2017b). NITI Aayog, the government's policy planning organisation, released a plan in July 2018 to create a National Health Stack (NHS), a digital framework that would serve as a platform integrating IT solutions for the health sector (NITI Aayog, 2018). It was envisaged as a tool that would rapidly digitise health in India and produce a culture of innovation around healthcare provision and management. NITI Aayog hopes that the NHS will reduce the costs of health provision and protection, and integrate disparate healthcare systems to produce a cashless and seamlessly integrated experience for Indian citizens. The NHS will have several components – India Stack, Electronic Health Registry, Coverage and Claims Protection, Digital Health ID, Federated Personal Health Records Framework and the National Health Informatics Framework (NITI Aayog, 2018). The design of the NHS facilitates the collection, processing and storage of healthcare data across India. This will create healthcare databases with aggregate data that could be deployed for public and private purposes. The kinds of health data that could be made available include specific medical histories, medication and allergy information, immunisation status, test results, vital signs, and personal information, including body condition, demographics and billing. Access to the data will allow health insurance providers to fine-tune the services they provide, while the digitalisation of processes will result in reduced costs of operations (NITI Aayog, 2018). The scope of the NHS is wide – it covers managing private hospital and practitioner administration, Non-Communicable Diseases, Disease Surveillance, Nutrition Management, Emergence Health Services, Tele-health, Diagnostics, Health Systems Management, etc. (NITI Aayog, 2018). The infrastructure is organised across two layers that revolve around data – the National Health Registries Layer, which houses the applications that manage the healthcare data, and another layer of software services that operationalise various programmes.

National Health Stack

Components:

- India Stack, Electronic
- Health Registry
- Coverage and Claims
- Protection
- Digital Health ID
- Federated Personal Health Records Framework
- National Health Informatics Framework

Facilitates:

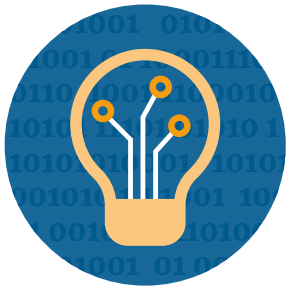
- Collection
- Processing
- Storage

Kinds of Data:

- Specific Medical Histories
- Medication and Allergy Information
- Immunisation Status
- Test Results
- Vital Signs
- Personal Information (Like Body Condition, Demographics and Billing)

Target:

- Fine-tune the Services
- Reduce Costs (e.g. Operations)



Data Cultures

The COVID-19 pandemic has transformed discussions around health data with the introduction of several contact-tracing applications to combat the spread of the coronavirus. Indian citizens appear to be losing the debate to manage and protect personal data as the interests and responsibilities of the state expand to manage unprecedented crises like a pandemic. For example, the digital contact-tracing app Aarogya Setu was meant to be consensual and voluntary, but it was later made mandatory for government employees and citizens living in containment zones. The app, which was developed by the government of India, has also raised key concerns about how it stores and shares the data it collects (Joshi, 2020).

Rules that were designed to protect against and deter cyber risks are being reframed or reconsidered given contingent public order and security concerns. Questions exist around the Personal Data Protection Bill and its enactment, which could create a broad framework that will apply to sectoral data guidelines. It is unlikely that any health policy framework being devised in the absence of a broader privacy protection framework will comply with the provisions of the PDP bill and the establishment of an independent data regulator – the Data Protection Authority (DPA).

One key issue and problem vis-à-vis data protection in India that surfaces as we consider sensitive health data is trust. Can citizens trust how their data is collected and used? Health data differs from other kinds of personal data because of its sensitive nature and the range of stakeholders involved – physicians, clinics, hospitals, patients, etc. So far, the policy thrust has been to create new registries and exchanges where health data can be shared and used. Policies like the National Health Stack and National Digital Health Mission largely function as platforms where citizens interact and transact with other healthcare providers through data. **Unlike the FinTech industry, which has been heavily regulated and where provisions to ensure confidentiality exist, the healthcare sector does not have rules governing the sharing of information. This vacuum engenders questions and concerns as health data gets digitised and shared without specific or overarching laws governing privacy and data protection or even sufficient rules with respect to confidentiality.** Moreover, awareness and cognisance of personal data issues does not exist in the health sector given how health has been provided for Indian citizens. Concerns around trust regarding health data have heightened after the release of the Non-Personal Data Committee report (2020), which called for anonymised data to be managed under the aegis of the government. Health data will likely be aggregated, segmented and anonymised to advance research and innovation and the health policy priorities of the government.

Law and Regulations

Public health issues are generally governed by comprehensive national health policies. India has had two such policies – 1983 and 2002. Both have served as blueprints to manage the expanding health sector. In 2017, the government introduced a new National Health Policy to manage new health challenges by prioritising them and allocating resources. The new health policy also identified a transformed health context marked by three changes – the rising burden of non-communicable diseases like heart disease, diabetes and cancer; the emergence of a robust private healthcare industry; and rising health expenditures as health challenges widen and the means to pay for them grow (Ministry of Health and Family Welfare, 2017b). The fundamental aim of NHP 2017 is to 'inform, clarify and strengthen' the role of the government in shaping health systems, policies and outcomes. One key component is to leverage and unlock the potential of digital health to improve the provision and delivery of care.

The NHP reiterates the ongoing push toward mainstreaming digital health through various policies. It calls for the establishment of a National Digital Health Authority (NDHA), suggested by a recent health data legislation, the DISHA, which will regulate, develop and deploy digital health across the healthcare system, particularly to improve healthcare outcomes given rising costs. A key means to achieve this end would be the establishment of digital health information infrastructures that collect and collate relevant health information and data and link existing public and private health systems through health registries. To facilitate these outcomes, health data must have adequate protections to deter theft and prevent breaches. Data breaches have increased in India, with confidential information being exposed or stolen. **Besides these risks, health data requires more protection so as to improve trust in the central government's ability to manage and run systems that standardise and control the process of collecting, storing, sharing and using health data.** The Ministry of Health and Family Welfare released a draft legislation, the Digital Information Security in Healthcare Act (DISHA), in March 2018, to legislate information security in the health sector, ensuring certain levels of privacy for citizens engaging the public health system (Ministry of Health and Family Welfare, 2017a). DISHA looks to accomplish this task using rules covering the collection, storage and transmission of digital health data enacted through a new National Digital Health Authority (NDHA).

Under DISHA, 'clinical establishments' or any organisation dispensing care as well as laboratories have the responsibility to secure personal health information (Ministry of Health and Family Welfare, 2017a). These establishments are primarily responsible for data security or the protection of an individual's digital healthcare data (DHD), which consists of an individual's electronic health records. The secure health information belongs to the individual who generates the DHD and who is recognised as the custodian of the data. The 'clinical establishment' thus retains the data as a trustee without ownership or transfer rights (Ministry of Health and Family Welfare, 2017a). Consent is required, as per the bill, before the collection of data occurs and the data is transferable only after encryption. Finally, the draft bill also calls for the establishment of a National Electronic Health Authority (NeHA) and State Electronic Health Authorities, which will promulgate standards and rules that oversee the processing of

digital health data with sufficient power to ensure compliance by relevant stakeholders (Wadhwa, 2020). Despite some comprehensive and novel provisions, DISHA has neither been passed nor deliberated upon in parliament. There is apprehension that the government's moves towards creating new digital health systems and apparatuses like the National Health Stack and National Digital Health Mission will be carried out in the absence of a law like DISHA or the Personal Data Protection Bill (2019) that protects the rights of users providing sensitive data. Civil society groups and privacy proponents have been urging the government to enact a comprehensive data protection framework before introducing and implementing policies that expand the government's widening digital footprint.

Conclusion

Questions around data protection are vital in India. Since 2017, the Indian government has been attempting to draft, negotiate and legislate a comprehensive data protection framework that would clarify and delineate the rights of citizens who provide data; firms and organisations who collect, store and process data; and the government, which acts to ensure this process comports with existing constitutional norms governing privacy and the rights and responsibilities of the state. It has been a fitful process, not least due to the politics around data and the preferences of a wide range of actors, both state and non-state. As India's digital economy grows, data-related issues will consume each sector as Indian citizens generate and provide bits and pieces of their personal information online. Concerns abound around a litany of issues related to data: Who owns the data? What protections do citizens have as they provide data to various firms and organisations or 'data fiduciaries'? How will the new data regulator govern data across sectors and industries? Will the state exempt itself from rules governing data? These concerns have been amplified by the COVID-19 pandemic, which has seen the government turn to digital tools and applications to mitigate and control outbreaks. This ongoing digital transformation has seeped across policy areas, including finance (FinTech) and health, which are covered in this report.

The extensive use of data in India and concerns about how it will be managed, controlled and monetised mean that perceptions of India's personal data landscape vary depending on who you approach and their relative inclinations and interests. Undeniably, **public concerns and qualms over personal information and data being collected are rising;** recent surveys indicate that Indian citizens are perturbed by how the government manages data they submit as they transact over various digital platforms (Karan, 2018). Public anxieties have been rising since the advent of India's Aadhaar programme, which provides every Indian citizen with a digital identity that allows them to transact digitally. **For government officials, however, data is a national asset that has to be strategically managed to advance developmental priorities. Data is conceptualised as a tool that can assist bureaucrats and policymak-**

ers to design policies, disburse welfare and subsidies, realign incentives, cut costs and provide services. Protecting data helps Indian policymakers fortify public digital infrastructures like Aadhaar and the related India stack apparatus that incentivises innovators and entrepreneurs to develop applications for public use; complete data access facilitates these outcomes. Such perceptions influence policy discussions and the unveiling of frameworks and policies concerning personal and non-personal data in the FinTech and health sectors. Such discussions have only amplified since the coronavirus crisis took hold.

The COVID-19 pandemic has battered India. The government acted quickly in March 2020 to prevent a major outbreak but the effort was largely in vain. The spread of the virus has also placed the government in a financial bind as the economy has slumped. With limited means to tackle the virus and the compelling need to physically distance, the government appears to have settled on relying on and leveraging digital applications, systems and services to not only manage the pandemic but also reorient policies in sectors that have not digitised. Health is one such area that has, of late, seen a flurry of policy activities. India's financial industry, however, has become more digital, building upon the government's digital infrastructures to create new pathways of engagement with a vast mobile customer base. **Yet, without a comprehensive data protection law that decrees how data will be regulated, the rights of citizens and the responsibilities of organisations and governments, the ongoing push to digitise and innovate in these and other policy areas will suffer. Trust will be eroded.** Such a scenario will not only complicate how India regulates data at home but also its position as an economy worthy of sustained investment, as economies around the world reorganise around the services industry.

REFERENCES

A **Ahluwalia, Shilpa** (2020). Aadhaar: The way forward for FinTech companies. *India Business Law Journal Online.* Retrieved from https://law.asia/aadhaar-FinTech-companies/.

Angell, B. J., Prinja, S., Gupt, A., Jha, V. & Jan, S. (2019). The Ayushman Bharat and the path to universal health coverage in India: Overcoming the challenges of stewardship and governance. *PLoS medicine,* 16(3): e1002759.

B **Basel Committee on Banking Supervision** (2018). *Implications of FinTech developments for banks and bank supervisors.* Retrieved from https://www.bis.org/bcbs/publ/d431.pdf.

Bhakta, Pratik (2018). India's FinTech companies struggle for an alternative to Aadhaar. *The Economic Times,* December 21. Retrieved from https://economictimes.indiatimes.com/small-biz/startups/features/indias-FinTech-companies-struggle-for-an-alternative-to-aadhaar/articleshow/67186586.cms.

Biospectrum Asia (2019). India hosts 4th Global Digital Health Partnership Summit. Biospectrum Asia, February 25. Retrieved from https://www.biospectrumasia.com/news/46/12885/india-hosts-4th-global-digital-health-partnership-summit.html.

C **Clarence, A.** (2020). Aarogya Setu: Why India's Covid-19 contact tracing app is controversial. *BBC News*, May 15. Retrieved from https://www.bbc.com/news/world-asia-india-52659520.

D **D'Silva, D., Filková, Z., Packer, F., and Tiwari, S.** (2019). *The Design of Digital Financial Infrastructure: Lessons from India*. BIS Papers, December 2019.

Department of Economic Affairs, Ministry of Finance (2017). Press Release on the Report of the Working Group for setting up Computer Emergency Response Team in the financial sector. June 30. Retrieved from http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

F **Future Health Index 2019** (2019). Philips. Retrieved from https://images.philips.com/is/content/PhilipsConsumer/Campaigns/CA20162504_Philips_Newscenter/Philips_Future_Health_Index_2019_report_transforming_healthcare_experiences.pdf.

G **Gill, Prabhjote** (2020). India's three main surveillance projects NATGRID, CMS and NETRA have been directed to stop collecting data citing breach of privacy. *Business Insider India*, December 2. Retrieved from https://www.businessinsider.in/tech/news/indias-three-main-surveillance-projects-natgrid-cms-and-netra-have-been-directed-to-stop-collecting-data-citing-breach-of-privacy/articleshow/79529256.cms.

Government of India (2000). Department of Parliamentary Affairs, 'Information Technology Act 2000'. Retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf.

Gupta, K. (2018). UPI 2.0 launched. Here are its key features. *Livemint,* August 2. Retrieved from https://www.livemint.com/Money/Cog3dAvOZka0OsNg8M9S8O/UPI-20-launched-Here-are-its-key-features.html.

I **India Brand Equity Foundation** (2020). *Indian Healthcare Industry Report.* Retrieved from http://www.ibef.org/industry/healthcare-india.aspx.

J **Invest India** (2020). *Financial Sector in India – Indian FinTech Industry Trends*. Retrieved from https://www.investindia.gov.in/sector/bfsi-FinTech-financial-services.

Joshi, D. (2020). India's digital response to COVID-19 risks creating a crisis of trust. *The Wire*, May 1. Retrieved from https://thewire.in/tech/covid-19-aarogya-setu-surveillance.

K **Kalra, A.** (2018). Exclusive: U. S. senators urge India to soften data localisation stance, *Reuters*, October 13. Retrieved from https://www.reuters.com/article/us-india-data-localisation-exclusive-idUSKCN1MN0CN.

Karan, K. (2018). Is privacy an elitist concern? Not so, says new survey. *Scroll.in*, November 14. Retrieved from https://scroll.in/article/899168/is-privacy-an-elitist-concern-not-so-says-new-survey.

Khushhal, K. (2020). National digital health mission puts the spotlight on India's health data security. *Financial Express*, September 29. Retrieved from https://www.financialexpress.com/lifestyle/health/national-digital-health-mission-puts-the-spotlight-on-indias-health-data-security/2094277.

M **Matthan, R., Venkataraman, M. & Patri, A.** (2017). *Privacy, Security and Ownership of Data in the Telecom Sector.* Policy Advisory, Takshashila Institution. Retrieved from https://trai.gov.in/sites/default/files/Takshashila_07_11_2017.pdf.

Ministry of Finance (2017). *Press Release on the Report of the Working Group for setting up Computer Emergency Response Team in the financial sector.* Department of Economic Affairs. June 30. Retrieved from http:// dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

Ministry of Health and Family Welfare (2017a). Digital Information Security in Healthcare Act [Draft for Public Consultation]. Government of India. Retrieved from https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf.

Ministry of Health and Family Welfare (2017b). National Health Policy 2017. Government of India. Retrieved from https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf.

Ministry of Health and Family Welfare (2019a). *MOHFW: E-health & Telemedicine.* Government of India. Accessed October 19, 2020. Retrieved from https://main.mohfw.gov.in/Organisation/departments-health-and-family-welfare/e-Health-Telemedicine.

Ministry of Health and Family Welfare (2019b). National Digital Health Blueprint. Government of India. Accessed October 17, 2020. Retrieved from https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf.

Ministry of Health and Family Welfare (2020). MOHFW: Departments of Health and Family Welfare. Retrieved from https://main.mohfw.gov.in/organisation/Departments-of-Health-and-Family-Welfare.

N **National Health Portal** (2020). *National Digital Health Mission (NDHM).* Government of India. Retrieved from https://www.nhp.gov.in/national-digital-health-mission-(ndhm)_pg.

National Payments Corporation of India (2018). Retail payments statistics on NPCI platforms. Accessed August 11, 2020. Retrieved from https://www.npci.org.in/sites/default/files/RETAIL%20PAYMENTS%20STATISTICS%20ON%20NPCI%20PLATFORMS%20-%20June%202018_1.pdf.

NITI Aayog (2018). National Health Stack: Strategy and Approach. Accessed October 13, 2020. Retrieved from https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf.

P **Pareek, M.** (2018). Ayushman Bharat–national health protection mission a way towards universal health cover by reaching the bottom of the pyramid – To be a game changer or non-starter. *International Journal of Advanced and Innovative Research,* 7(7), pp. 1–10.

Patil, S. & Chakraborty, S. (2019). *A Cybersecurity Agenda for India's Digital Payment Systems.* Gateway House. Retrieved from https://www.gatewayhouse.in/wp-content/uploads/2019/10/Digital-Payments_FINAL.pdf.

PricewaterhouseCoopers (2016). *Indian healthcare on the cusp of a digital transformation.* Retrieved from https://www.pwc.in/assets/pdfs/publications/2016/indian-healthcare-on-the-cusp-of-a-digital-transformation.pdf.

R **Reserve Bank of India** (2016). *Cyber Security Framework in Banks.* Retrieved from https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=10435.

Reserve Bank of India (2018a). Report of the Working Group on FinTech and Digital Banking. Retrieved from https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=892.

Reserve Bank of India (2018b). *Storage of Payment System Data*. Retrieved from https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

Reserve Bank of India (2019). *Report of the High Level Committee on Deepening of Digital Payments*. Retrieved from https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CDDP03062019634B0EEF3F7144C3B65360B280E420AC. PDF.

S **Sarbadhikari, S. N.** (2019). Digital health in India – As envisaged by the National Health Policy. *BLDE University Journal of Health Sciences,* 4(1), pp.1–6.

Singh, S. & Porecha, M. (2020). *Behind the rush and hush of India's National Digital Health Mission.* The Ken. Retrieved from https://the-ken.com/story/behind-the-rush-and-hush-of-indias-digital-health-mission/.

Singhal, A. (2019). *Mumbai Thrives to Become the FinTech Hub.* Entrepreneur India. Retrieved from https://www.entrepreneur.com/article/333951.

T **Tandon, A.** (2021). *6.3 lakh digital health IDs generated.* The Tribune. Retrieved from https://www.tribuneindia.com/news/nation/6-3-lakh-digital-health-ids-generated-207154.

Telecom Regulatory Authority of India (2020). *Highlights of Telecom Subscription Data as on 31 March 2020*. Press Release no. 49/2020.

U **Unique Identification Authority of India** (2019). *Now 125 Crore Residents of India have Aadhaar*. Press Release. December 31.

U.S. Food and Drug Administration (2020). *What is Digital Health*? Government of the United States. Retrieved from https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health.

V **Vir, A. and Rahul, S.** (2020). "The Internet Country: How India created a digital blueprint for the economies of the future" *Tigerfeathers*, February 21. Retrieved from https://tigerfeathers.substack.com/p/the-internet-country, February 21, 2020/.

W **Wadhwa, M.** (2020). *National eHealth Authority (NeHA).* ICT India Working Paper #29. Centre for Sustainable Development, Columbia University. Retrieved from https://csd.columbia.edu/sites/default/files/content/docs/ICT%20India/Papers/ICT_India_Working_Paper_29.pdf.

X **Xynou, M.** (2014). *India's Central Monitoring System (CMS): Something to worry about?* Centre for Internet and Society. Retrieved from https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

Sample of Questions

Semi-structured interviews were conducted with questions broadly aligned with three themes:

1. How the regulation of data affects innovative capacities
2. Data cultures, or perceptions around data and innovation
3. How data creates value or values

A sample of questions for each theme follows:

Regulation	• To what extent do you think the laws and regulations around data protection have been helping or hindering the innovation capabilities of firms and organisations? • Do you see the legal landscape, as in the laws and regulations in specific, or the legal framework, changing in the next few years? • How can the current laws and regulations, including the legal framework, be improved so that the innovation capabilities of organisations can be further enhanced?
Data cultures	• How is personal data seen in India? For example, do people see it as something that they need to protect? Or as byproducts of economic transactions? • How might perceptions of personal data and privacy have an impact on innovation? For example, what types of data would be considered taboo to share, and in what contexts?
Data and value creation	• What do you think is the value that organisations bring when they are successful in managing their data, including analysing, storing, protecting, and sharing their data? • How do you think frameworks like the GDPR affect domestic and trans-border operations, and to what extent do you think a similar framework would be feasible in India?

Methodology

The overall methodology of this project is based on a case study approach, in order to deepen insights into the topic in the different domains of FinTech and health. Following case study best practices, we collect our data from multiple sources (Eisenhardt 1989; Yin 2014); in this case, through semi-structured expert interviews, podcasts and published documents.

Research was completed through a triangulation of semi-structured interviews and document analysis. Fifteen interviews were conducted with members of the public, the private sector and civil society, including participants with different areas of expertise, such as lawyers, social scientists, entrepreneurs and public policy analysts. All the interviews were carried out over online calls given public health restrictions that barred travel. Interview questions were modified based on the expertise of each interviewee, but largely focused on three broad concerns: perceptions of data held by various public and private actors, including stakeholders in innovation ecosystems; how these perceptions influenced policy discussions around data; and the extent to which these discussions advance innovation. In addition to the interviews, references were made to 60 publicly available materials, including reports from businesses, commentaries and insights from legal analysts, government documents and two podcasts that senior Indian government officials gave when the Indian government was deliberating on how to legislate data. All interviews were recorded with permission, transcribed and analysed with the documents using thematic analysis.

AUTHORS

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies, National University of Singapore.

Dr Natalie Pang is a scholar of digital humanities, specialising in socio-technical studies of technology including social media and civil society and the convergence of data and AI in urban cities.

Wong Kwang Lin is a researcher with a background in anthropology, with an interest in issues including digital justice, urban spaces and heritage, and migrant advocacy.

Editors
Christian Echle
Director Regional Programme Political Dialoge Asia
christian.echle@kas.de

Katharina Naumann
Desk Officer for International Media Programmes
katharina.naumann@kas.de

Konrad-Adenauer-Stiftung e. V.
Regional Programme Political Dialogue Asia
Arc 380
380 Jalan Besar, #11-01
Singapore 209000
www.kas.de/singapore

Imprint

Published by:
Konrad Adenauer Stiftung Regional Programme
Political Dialogue Asia, Singapore, 2021

Design and typesetting: yellow too Pasiek Horntrich GbR

Printed with financial support from the German Federal Government.

ISBN 978-981-18-4822-3

Data fuels digital change. The ability to collect, process, and make available ever-increasing amounts of data is a key to innovation and growth.

This report is one of the series surveying seven different Asian territories to deepen understandings of innovation and data policies, and contribute to debates about data governance and data protection. The study was carried out in collaboration with the National University of Singapore (NUS). We selected Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan as the contexts to be examined. We looked at the areas of transport, finance, administration, health and smart cities to understand how innovation is driven in the context of relationships among key stakeholders such as citizens, civil societies, government agencies, private sectors and research institutions.

This report focuses on two policy areas in India where innovation has occurred in the absence of a comprehensive data protection law that could affect how governments, firms, organisations and individuals interact for personal and commercial purposes. Through the key cases covered in this report – in the finance and health domains – we also consider and unpack how different actors operate and innovate in a policy vacuum.

Konrad-Adenauer-Stiftung e. V.

DATA AND INNOVATION IN ASIA-PACIFIC