S&R

Data+

India's Proposed Digital Governance Framework: Past Developments and Present Status

This is the second note of ***S&R Data+***, a multipart series on data governance, focused on distinguishing between personal and non-personal information, including with respect to their separate regulatory, legal, and commercial implications. The previous note summarized India's existing data protection framework and provided an overview of India's legislative trajectory in that regard. Here, we provide a snapshot of the gradual build-up to India's proposed digital governance framework by analyzing past trends which have led to present developments. In the next note, we will discuss possible trajectories for the future in respect of such governance regime, including in the context of data localization.

While a recent flurry of legislative and policy activity promises to transform the country's digital future, two landmark laws with respect to digitized personal and non-personal data, respectively, may attain concrete shape by the end of 2023 itself – thereby replacing India's existing data protection framework under the Information Technology Act, 2000, as amended, along with its allied rules.

The Past

Back in 2017, a white paper on a revised data protection framework for the country (the "**White Paper**"), as released by a government-constituted expert committee ("**Expert Committee**"), had acknowledged the presence of new technologies, such as the Internet-of-Things ("**IoT**"), which rely on the continuous collection of personal information from users of 'smart' devices. Such information, in turn, may be subsequently (re)interpreted to provide unique services. Further, the White Paper had noted that it was often difficult to distinguish between personal and non-personal data for data localization purposes. Further, a majority of commenters, including major technology companies, had suggested that mandatory data localization would have an adverse impact on industry.

In addition, the White Paper had recognized that cross-border data transfers involved international cooperation in data processing, storage, and transmission. Since rapid data movements across the globe had served as a key foundation for building the international economic order, the Expert Committee had opined that localization norms would restrict such movement, posing obstacles for companies across sectors.

Nevertheless, in its report on a free and fair digital economy, submitted in July 2018 pursuant to stakeholder feedback (the "**EC Report**"), the Expert Committee had recognized the emergence of activities involving data processing which held considerable strategic and economic interest for the country, especially with respect to non-personal data. Meanwhile, Clause 105 ("*No application to non-personal data*") of the draft Personal Data Protection Bill, 2018 ("**PDP 18**"), which the Expert Committee had presented along with the EC Report, specified that nothing contained in the former would affect the power of the central government to formulate appropriate policies for the digital economy – including in respect

of measures adopted for its growth, security, integrity, etc. – as long as such policies/measures did *not* govern personal data.

Further, a detailed report was submitted by a joint committee, to which PDP 18's next iteration – the Personal Data Protection Bill, 2019 ("**PDP 19**") – had been referred at the time of the latter's parliamentary introduction a year and a half after the EC Report was released, based on the recommendations of the Expert Committee and suggestions from various stakeholders (such joint committee, the "**Joint Committee**," and its report, the "**JC Report**"). While PDP 19 was introduced in, and withdrawn from, Indian parliament in December 2019 and August 2022, respectively, the JC Report, as presented before parliament in December 2021, had recommended that PDP 19 should deal with both personal and non-personal data. Moreover, it was suggested that the short title of PDP 19 ought to be changed to the 'Data Protection Act, 2021' ("**Proposed DP Act**"). Further, the JC Report proposed the establishment of an alternative financial system in India.

Noting that privacy had been widely compromised via the SWIFT network – through the use of which Indian citizens were engaged in significant cross-border payments – the Joint Committee acknowledged that data protection in the financial sector was a matter of global concern. Accordingly, it was of the view that an alternative to the SWIFT payment system ought to be developed in India (such as Ripple in the US, or INSTEX in the EU), which could provide a boost to the domestic economy along with ensuring privacy.

Another key recommendation made in the JC Report was in respect of digital devices and equipment that related to IoT. PDP 19 had contained no provision for regulating hardware manufacturers which collected data through digital devices and software. Accordingly, the JC Report recommended the addition of Clause 49(2)(o) of the Proposed DP Act to enable the proposed data protection authority to frame such regulations as required in the future. The Joint Committee further recommended that a formal certification process could be established with respect to: (i) digital and IoT devices for ensuring data security; and (ii) emerging technologies with the potential to train AI systems. For the purpose of achieving these objectives, the Joint Committee suggested that the Indian government should set up a nationwide network of dedicated laboratories or testing facilities which could provide certifications in respect of the integrity and security for all digital devices.

Although such recommendations were similar to contemporaneous discussions in Europe with respect to regulating IoT-related data for the purpose of improving data utilization, the focus in the JC Report restricted itself to the possibility of malicious insertions in the underlying hardware/software that might cause data breaches.

Finally, with the aim of gradually introducing data localization, the Joint Committee suggested that a policy in this regard ought to include aspects such as the development of adequate infrastructure for the safe storage of citizens' data, support for local businesses and start-ups to comply with such data localization norms, proper taxation of data flows, as well as creation of a local AI ecosystem. In this regard, the committee had further recommended that steps taken by the government towards this objective should guarantee the ease of doing business and promote initiatives such as 'Digital India'.

However, in contrast to the Joint Committee's recommendation about including both personal and non-personal data within the same statute – and on account of lingering uncertainties about the advisability of such a move – the Ministry of Electronics and Information Technology ("**MeitY**") had constituted a separate

committee of experts in September 2019, *i.e.*, a couple of months before the establishment of the Joint Committee, to deliberate on a framework for data governance (the "**DG Committee**"). In particular, the DG Committee was mandated to: (a) study various issues relating to non-personal data; and (b) make specific suggestions with respect to regulating non-personal data.

As part of its deliberations, the DG Committee met with representatives from various business sectors, including Indian and foreign companies with global operations, to obtain an assortment of industry opinion on topics such as health, e-commerce, and technology. In addition, separate subject-matter experts were invited to present and discuss their views with the DG Committee. A draft version of the DG Committee's first report was released in July 2020 (the "**First DGC Report**"), inviting comments from the public.

Among other things, the First DGC Report analyzed the socio-economic impacts of abundantly available data, which in turn was found to be creating a market imbalance. Since such data was not being used optimally – especially for socioeconomic and public purposes – the DG Committee concluded that there was a clear need for regulating such data.

Accordingly, the First DGC Report provided a definition of non-personal data and divided such data into three categories involving public, community, and private perspectives, respectively. Further, with regard to non-personal data in particular, it defined key roles (such as data principal, data custodian, and data trustee) and an institutional form of data infrastructure (data trust). Further, in terms of ownership, the First DGC Report articulated a legal basis for establishing rights over non-personal data. In addition, it defined a 'data business' and discussed the requirements with regard to such business in terms of registration and data disclosure.

In this regard, the First DGC Report noted that in the global data economy, the proliferation of big data analytics and AI had led to the creation of information-intensive services where the underlying data interactions exert the greatest effect on value creation. Thus, a new category of business – a 'data business' – was envisaged as one that collects, processes, stores, or otherwise manages information, and meets certain threshold criteria. Thus, many existing businesses across several sectors which collect data beyond a threshold level may get categorized as a data business in the future. Within India, such data businesses can provide open access to meta-data, as well as regulated access to its underlying data.

Furthermore, the First DGC Report articulated the main motivations behind data sharing and recommended mechanisms for such sharing. In that regard, it proposed a separate legislation to govern and regulate non-personal data, including through the establishment of a 'Non-Personal Data Authority' ("**NPDA**") and by following certain technology-related guidelines for digitally implementing the recommended rules around data sharing.

Pursuant to its review of the feedback received to the First DGC Report, the DG Committee proposed a revised version of such report (the "**Revised DGC Report**") a few months later. In terms of revision, the DG Committee: (i) clarified the definition of non-personal data, and (ii) re-examined the legal basis for asserting sovereign and community rights over non-personal data. It also expanded on the idea of high-value datasets, along with a data trustee that manages such datasets, and differentiated the roles of a data custodian and a data processor.

Even while providing recommendations about data sharing for a 'public good' purpose, the DG Committee recognized the presence of pre-existing practices among private organizations with respect to the sharing of data for the purpose of boosting profits. Accordingly, it made no recommendations towards such

business-related data sharing. However, it did retain certain key features of the First DGC Report, including those related to consent requirements for anonymized data, data businesses, and an NPDA.

Later in the ***S&R Data+*** series, we will: (i) discuss how recent legislative and regulatory efforts in India have sought to deal with anonymization and anonymized data; and (ii) examine in greater detail some of the key discussions around non-personal and anonymized data, including with reference to the First and Revised DGC Reports, respectively.

The Present

The definition of 'data' in Clause 3(13) of PDP 18 – similar to the one contained in Clause 2(4) of India's current draft of the Digital Personal Data Protection Bill, 2022 ("**DPDP**") – included a reference to the processing of data by 'automated means,' which term referred to any equipment capable of operating automatically in response to instructions given for the purpose of processing data (see Clause 3(7) of PDP 18). In turn, DPDP defines 'data' in a manner more or less consistent with its equivalent under Section 2(1)(o) of the Information Technology Act, 2000, as amended (the "**IT Act**") – albeit including additional components such as automated processing.

In that regard, 'automated' has been defined in Clause 2(1) of DPDP as "any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data." Furthermore, Clause 4(1) of DPDP ("*Application of the Act*") limits the operation of the proposed data protection framework to the processing of *digital* personal data within Indian territory (collected online or offline, as long as such personal data has been digitized). In addition, DPDP applies to the processing of digital personal data *outside* Indian territory when such processing relates to the profiling of – what it terms – a 'data principal.' According to Clause 2(6) of DPDP, a data principal is the individual with respect to whom certain personal data relates. The EU's General Data Protection Regulation ("**GDPR**") uses the term 'data subject' to mean the same thing.

Apparently inspired by Article 4(4) of GDPR, Clause 4(2) of DPDP refers to 'profiling' as any form of processing of personal data that analyzes or predicts certain aspects related to the behavior, attributes, or interests of a data principal. Meanwhile, 'processing' itself has been defined in Clause 2(16) of DPDP as a set of automated operations performed on digital personal data. Accordingly, Clause 4(3)(a) clarifies that DPDP does *not* apply to the *non*-automated processing of personal data, and Clause 4(3)(b) further specifies that it does not apply to offline personal data either, if such data is subsequently left undigitized. Similarly, Article 2(1) ("*Material Scope*") of GDPR makes it clear that it does not apply to the non-automated processing of personal data which is not intended to be part of a 'filing system'. Article 4(6) of GDPR defines a 'filing system' as any structured set of personal data which is accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis.

Further, the explanatory note to DPDP, which accompanied the draft's release in November 2022, specified that India's proposed law will only apply to digital personal data in recognition of the rising role of the internet and increased digitalization. Accordingly, to maintain its focus on the digital nature of interactions within the context of widespread digitization across the Indian economy, DPDP recognizes that information in general, and personal data in particular, remains at the core of a fast-growing ecosystem of digital products, services, and intermediation.

While ‘digitization’ refers to the process of converting physical or analog information (such as paper documents or images) into digital, machine-readable formats which may be accessed, stored, and manipulated using computers and digital technologies, ‘digitalization’ refers to the use of digital technologies (such as cloud computing, artificial intelligence, and IoT) to automate and/or otherwise improve upon business processes, create additional value for customers through new products and services, enhance customer experience, as well as generate revenue. Thus, digitization is the first step towards digitalization. In other words, by converting physical data into digital formats, businesses can better leverage digital technologies.

The Future

While the Indian government’s ‘Digital India’ initiative involves the digitization of data across governance, healthcare, education, payment systems, as well as online transactions in general, Clause 18(2) of DPDP grants important exemptions to the government and state instrumentalities. Further, Clause 18(4) read with Clause 9(6) of DPDP suggests that a government body which processes personal data may retain such data, as well as the means through which such data can be associated with particular individuals, even after retention is unnecessary in terms of the original purpose of collection, or for legal and business purposes.

While recent media reports suggest that a (potentially) revised version of DPDP, pursuant to stakeholder feedback, is likely to be tabled before parliament in the month of July, a proposed ‘Digital India Act’ (“**Proposed DI Act**”) has also gathered considerable regulatory and consultative traction – further to which a draft bill is expected to be made ready around the same time. Thus, July promises to be a significant period for the country’s future.

In the next note, we will examine the possible impact of such present developments, including with respect to the National Data Governance Framework Policy and the Proposed DI Act, on the shape of laws to come. We will also trace the contested legislative trajectory of data localization.

*This insight has been authored by **Deborshi Barat** (Counsel); he can be reached at dbarat@snrlaw.in for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

S&R ASSOCIATES ADVOCATES

NEW DELHI
64 Okhla Industrial Estate
Phase III
New Delhi 110 020
Tel: +91 11 4069 8000

MUMBAI
One World Center, 1403 Tower 2 B
841 Senapati Bapat Marg, Lower Parel
Mumbai 400 013
Tel: +91 22 4302 8000