CARNEGIE INDIA

WORKING PAPER

OCTOBER 2023

Understanding India's New Data Protection Law

Anirudh Burman

Understanding India's New Data Protection Law

Anirudh Burman

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, D.C. 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

Carnegie India
Unit C-5 & C-6, Edenpark,
Shaheed Jeet Singh Marg
New Delhi – 110016, India
P: +011 4008687
CarnegieIndia.org

This publication can be downloaded at no cost at CarnegieIndia.org

Contents

Introduction

In early August 2023, the Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, 2023.[1] The new law is the first cross-sectoral law on personal data protection in India and has been enacted after more than half a decade of deliberations.[2] The key question this paper discusses is whether this seemingly interminable period of deliberations resulted in a "good" law—whether the law protects personal data adequately, and in addition, whether it properly balances, as the preamble to the law states, "the right of individuals to protect their personal data" on one hand and "the need to process such personal data for lawful purposes" on the other.

To answer this question, the paper first details the key features of the law and compares it to earlier versions, especially the previous official bill introduced by the government in Parliament in 2019.[3] The second part of the paper then examines the DPDP Act from two perspectives. First, it highlights certain potentially problematic features of this law to understand its consequences for consumers and businesses as well as the Indian state. Second, it places the act in context of the developments and deliberations that have taken place over the last five years or so. The third part speculates on the key factors that will influence the development of data protection regulation in India in the next few years.

The 2023 act is the second version of the bill introduced in Parliament, and fourth overall. An initial version was prepared by a committee of experts and circulated for public feedback in 2018.[4] This was followed by the government's version of the bill that was introduced in Parliament in 2019—the Personal Data Protection Bill, 2019. This version was studied by a parliamentary committee that published its report in December 2021.[5] The government, however, withdrew this bill, and in November 2022, published a fresh draft for public

consultations—the draft Digital Personal Data Protection Bill, 2022.[6] This draft was quite different compared to the previous versions. The 2023 law is based, in significant part, on this draft. However, it has some new provisions that are consequential for the questions this paper seeks to answer.

These four drafts were preceded by a landmark 2017 judgment by India's Supreme Court in *Justice K.S. Puttaswamy and Anr. v. Union of India and Ors*.[7] The judgment declared that the right to privacy is part of the fundamental right to life in India and that the right to informational privacy is part of this right. The judgment, however, did not describe the specific contours of the right to informational privacy, and it also did not lay down specific mechanisms through which this right was to be protected.

Following this, the first government version of the law, the Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019. This version was expansive in scope and proposed cross-sectoral, economy-wide data protection regulation to be overseen by an all-powerful data protection regulator—the Data Protection Authority (DPA). The 2019 bill provided for a preventive framework.[8] It imposed a number of obligations on entities collecting personal data—to provide notice and take consent from individuals, to store accurate data in a secure manner, and to use it only for purposes listed in the notice. Businesses were also required to delete data once the purpose was satisfied and to provide consumers rights to access, erase, and port their data. Businesses were required to maintain security safeguards and transparency requirements, implement "privacy by design" requirements, and create grievance redress systems. Finally, this bill introduced an entity known as "consent managers," who were intermediaries for collecting and providing consent to businesses on behalf of individuals.[9]

The bill grouped personal data into different categories and required elevated levels of protection for "sensitive" and "critical" personal data. Certain businesses were also to be categorized as "significant data fiduciaries," and additional obligations were proposed for them—registration in India, data audits, and data impact assessments. In addition, the bill imposed localization restrictions on the cross-border flows of certain categories of data. The DPA was empowered to impose penalties on businesses for violating these requirements. The bill also proposed to criminalize activities related to the deanonymization of individuals from anonymized datasets.

The 2019 bill exempted certain entities and businesses from notice and consent requirements under certain circumstances—for lawful state functions, medical and health services during emergencies or epidemics, breakdown of public order, employment-related data processing, the prevention and detection of unlawful activity, whistleblowing, and credit recovery, among others.

The 2019 bill also had a provision to empower the government to regulate nonpersonal data. It allowed the government to require private entities to hand over specific nonpersonal data that the government asked for as per conditions it prescribed. In short, the 2019 bill

proposed a comprehensive, cross-sectoral framework based on preventive requirements for businesses (defined as "data fiduciaries") and rights for individuals or consumers ("data principals").

This regulatory structure was based mostly on the 2018 draft bill proposed by the Srikrishna Committee—the committee, chaired by Justice B.N. Srikrishna, a retired Supreme Court judge, was set up by the Ministry of Electronics & Information Technology in July 2017 to help frame data protection norms. The recommendations of this committee, in turn, were based on major regulatory developments that were popular while the work of the committee was proceeding. Primary among these was the European Union's (EU's) General Data Protection Regulation (GDPR).[10] While the general preventive framework of the 2019 bill was welcome, its expansive scope was problematic. It created a number of significant compliance requirements that would have affected both big and small firms in the economy. It also proposed the creation of a DPA that had significant regulation-making and supervisory powers. These regulations would have further detailed the already significant compliance requirements in the bill. The novelty of the law and the lack of prior experience in implementing a data protection law of this nature would have created serious risks of overregulation or under-regulation.[11]

The DPDP Act is based on the draft proposed by the government in November 2022, which adopted a radically different approach to data protection regulation.[12] The next section details the key provisions of the act.

Key Features of the DPDP Act, 2023

Compared to the 2019 version of the bill, the DPDP Act, 2023 is more modest—it has reduced obligations for businesses and protections for consumers. On the one hand, the regulatory structure is simpler, but on the other, it vests the central government with unguided discretionary powers in some cases.

Applicability to Nonresidents

The DPDP Act applies to Indian residents and businesses collecting the data of Indian residents. Interestingly, it also applies to non-citizens living in India whose data processing "in connection with any activity related to offering of goods or services" happens outside India.[13] This has implications for, say, a U.S. citizen residing in India being provided digital goods or services within India by a provider based outside India.

Purposes of Data Collection and Processing

The 2023 act allows personal data to be processed for any lawful purpose.[14] The entity processing data can do so either by taking the concerned individual's consent or for "legitimate uses," a term that has been explained in the law.

Consent must be "free, specific, informed, unconditional and unambiguous with a clear affirmative action" and for a specific purpose. The data collected has to be limited to that necessary for the specified purpose. A clear notice containing these details has to be provided to consumers, including the rights of the concerned individual and the grievance redress mechanism. Individuals have the right to withdraw consent if consent is the ground on which data is being processed.

Legitimate uses are defined as: (a) a situation where an individual has voluntarily provided personal data for a specified purpose; (b) the provisioning of any subsidy, benefit, service, license, certificate, or permit by any agency or department of the Indian state, if the individual has previously consented to receiving any other such service from the state (this is a potential issue since it enables different government agencies providing these services to access personal data stored with other agencies of the government);[15] (c) sovereignty or security; (d) fulfilling a legal obligation to disclose information to the state; (e) compliance with judgments, decrees, or orders; (f) medical emergency or threat to life or epidemics or threat to public health; and (g) disaster or breakdown of public order.[16]

Rights of Users/Consumers of Data-Related Products and Services

The DPDP Act also creates rights and obligations for individuals.[17] These include the right to get a summary of all the collected data and to know the identities of all other data fiduciaries and data processors with whom the personal data has been shared, along with a description of the data shared. Individuals also have the right to correction, completion, updating, and erasure of their data. Besides, they have a right to obtain redress for their grievances and a right to nominate persons who will receive their data.

Obligations on Data Fiduciaries

Entities responsible for collecting, storing, and processing digital personal data are defined as data fiduciaries and have defined obligations. These include: (a) maintaining security safeguards; (b) ensuring completeness, accuracy, and consistency of personal data; (c) intimation of data breach in a prescribed manner to the Data Protection Board of India (DPB); (d) data erasure on consent withdrawal or on the expiry of the specified purpose; (e) the data fiduciary having to appoint a data protection officer and set up grievance redress mechanisms; and (f) the consent of the parent/guardian being mandatory in the case of children/minors (those under eighteen years of age). The DPDP Act also states that any

processing that is likely to have a detrimental effect on a child is not permitted. The law prohibits tracking, behavioral monitoring, and targeted advertising directed at children.[18] The government can prescribe exemptions from these requirements for specified purposes. This is potentially a problem since the powers to exempt are broad and without any guidelines.

While the 2023 act retains the broad categories of obligations for the most part, the key difference from the 2019 bill is the absence of the scope for the regulator, the DPA, to make detailed regulations on these obligations. In addition, the substantive requirements under each of these categories have been reduced.

There is an additional category of data fiduciaries known as significant data fiduciaries (SDFs). The government will designate data fiduciaries as SDFs based on certain criteria—volume and sensitivity of data and risks to data protection rights, sovereignty and integrity, electoral democracy, security, and public order.[19]

SDFs will have additional obligations that include: (a) appointing a data protection officer based in India who will be answerable to the board of directors or the governing body of the SDF and will also serve as the point of contact for grievance redressal; and (b) conducting data protection impact assessments and audits and taking other measures as prescribed by the government. The 2019 bill required that SDFs register in India. This requirement has been removed from the 2023 act.

Moderation of Data Localization Requirements

The 2023 law reverses course on the issue of data localization. While the 2019 bill restricted certain data flows, the 2023 law only states that the government may restrict flows to certain countries by notification. While this is not explicit, the power to restrict data flows seems to be to provide the government necessary legal powers for national security purposes. The law also states that this will not impact measures taken by sector-specific agencies that have or may impose localization requirements. For example, the Reserve Bank of India's localization requirements will continue to be legally valid.

Exemptions From Obligations Under the Law

The law provides exemptions from consent and notice requirements as well as most obligations of data fiduciaries and related requirements in certain cases: (a) where processing is necessary for enforcing any legal right or claim; (b) personal data has to be processed by courts or tribunals, or for the prevention, detection, investigation, or prosecution of any offenses; (c) where the personal data of non-Indian residents is being processed within India; and so on.[20]

In addition, the law exempts certain purposes and entities completely from its purview.[21] These include:

1. Processing in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognizable offense. This will allow investigative and security agencies to remain outside the purview of this law.

2. Data processing necessary for research, archiving, or statistical purposes if the personal data is not to be used to take any decision specific to a data principal.

3. The government can exempt certain classes of data fiduciaries, including startups, from some provisions—notice, completeness, accuracy, consistency, and erasure.

4. One problematic provision allows the government to, "before expiry of five years from the date of commencement of this Act," declare that any provision of this law shall not apply to such data fiduciary or classes of data fiduciaries for such period as may be specified in the notification. This is a significant and wide discretionary power and is not circumscribed by any guidance on the basis for such exemption, the categories that may be exempted, and the time period for which such exemptions can operate.

New Regulatory Structure for Regulating Data Privacy

The 2023 law completely changes the proposed regulatory institutional design. The 2019 bill proposed an independent regulatory agency. The DPA was proposed on the lines of similar government agencies in many EU countries that function independently of government and implement the GDPR. The proposed Indian DPA was arguably more powerful since it was proposed to have much more extensive regulation-making powers than DPAs under the GDPR. In addition to framing regulations, the DPA would have been responsible for framing codes of conduct for businesses, investigating cases of noncompliance, collecting supervisory information, and imposing penalties on businesses.

In contrast, the 2023 law establishes the DPB.[22] The board is not a regulatory entity and is very different from the DPA. Compared to the latter, the board has a limited mandate to oversee the prevention of data breaches and direct remedial action and to conduct inquiries and issue penalties for noncompliance with the law.[23] The board does not have any powers to frame regulations or codes of conduct or to call for information to supervise the workings of businesses. It can only do so during the process of conducting inquiries.

The members of the board will be appointed by the government, and the terms and conditions of their service will be prescribed in rules made by the government.[24] The law states that these terms and conditions cannot be varied to a member's disadvantage during their tenure.

The law allows the board to impose monetary penalties of up to 250 crore rupees (approximately $30.5 million).[25] Appeals from the board's orders will go to an existing tribunal— the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). In addition to monetary penalties, the bill allows data fiduciaries to provide voluntary undertakings to the board as a form of settlement of any complaints against them.[26] Therefore, the board is a very different institution in design compared to the DPA.

Finally, the 2023 law contains a novel provision not included or discussed in any previous version. This is Section 37, which allows the government, based on a reference from the board, to block the public's access to any information that enables a data fiduciary to provide goods or services in India. This has to be based on two criteria: (a) the board has imposed penalties against such data fiduciaries on two or more prior occasions, and (b) the board has recommended a blockage. The government has to provide the data fiduciary an opportunity to be heard before taking such action.

Analyzing the DPDP Act, 2023

This section analyzes the 2023 act from two perspectives. First, it explains the broad structure of the law and highlights its key features and issues. Second, it contextualizes the law in the background of the different drafts proposed before this and elaborates upon the deliberations that have led to it.

How Well Does the DPDP Act, 2023, Protect Privacy?

The 2023 act creates, for the first time, a data privacy law in India. It requires consent to be taken before personal data is processed and provides a limited number of exceptions that are clearly enumerated in the law. It provides consumers the right to access, correct, update, and erase their data, in addition to a right to nomination. It creates additional safeguards for the processing of children's data. For businesses, it creates purpose limitations and obligations to provide notice of data collection and processing and mandates security safeguards. The law requires the creation of grievance redress mechanisms by businesses. The DPB will also handle complaints and grievances and is empowered to issue penalties for noncompliance with the law.

For the first time, therefore, India has a statutory framework for data protection. The presence of the law will gradually lead to the development of minimal standards of behavior and compliance among businesses that collect data. In this regard, the approach of the government toward implementing and enforcing the law will be the critical variable—for example, whether implementation will be focused on data-heavy businesses or across the economy would be an important factor.

However, other than open questions related to implementation, there are some concerns with different provisions of the law and their potential for undermining the protections seemingly accorded in it.

First, the exceptions carved out for consent empower the state significantly and place state imperatives on a different pedestal compared to private entities. While this may be truly legitimate in some circumstances, like disasters or emergencies, the law enlarges the scope of such circumstances. For example, Section 7(b) of the law enables the government to sidestep consent requirements where a government service beneficiary has previously consented to receiving any other benefit from the state. While this may allow easier access to personal data of beneficiaries for receiving government services, it also creates a potential for the government to aggregate databases. This is because making true use of the potential of this provision would mean that government agencies would have to be exempted from purpose limitations that require personal data to be deleted after the purpose of the data has been satisfied.

Another example of this is the set of exemptions to the state for investigative, prosecutorial, and national security purposes. In Section 17(1)(c), the law exempts the requirements of notice and consent, among others, for the purposes of processing for "prevention, detection, investigation or prosecution of any offence or contravention of any law."[27] While this is understandable, Section 17(2)(a) subsequently provides a blanket exemption from the whole law to any government agency that the government may notify, in the interests of sovereignty, security, integrity, public order, and preventing incitement. Given the fact that Section 17(1)(c) already exists, Section 17(2)(a) only indicates the desire of Parliament to ensure a complete non-application of the data protection law to certain state agencies.

Provisions like these create a separate category of activity that is beyond the purview of data privacy requirements. It is problematic that the Indian state is not subject to many of the constraints that private entities are, especially in cases where there is no pressing requirement for such an exception.

Second, the discretionary rule-making powers that the government has under the law could, in some cases, undermine the protections provided in the law. For example, under Section 17(5), the government has the power to declare that any provisions of this law will not apply to any business or class of businesses within five years of the commencement of the law. There is no time frame for the operation of this exemption or any guidance on how this provision is to be used. An optimistic interpretation of this provision would suggest that this could be used to allow sunrise industries or startups some time to comply with the law. However, provision for this has already been made in Section 17(3), which provides limited exemptions to startups and other industries the government may notify. Therefore, Section 17(5) could potentially be used in a manner that defeats the purpose of the law. It is worth reiterating that the law only limits the government's power to give these exemptions for an initial period of five years. It does not provide any limit on how long these exemptions can last for.

Similarly, the government has some unguided rule-making powers for exempting businesses from certain requirements regarding the processing of children's data. Sections 9(1) to 9(3) specify certain requirements for the same—they require parental consent and prohibit profiling, among others. Section 9(4) allows the government to exempt any business or class of businesses from Sections 9(1) to 9(3) "subject to such conditions, as may be prescribed." This provision, again, fails to indicate on what grounds this exemption will be given, how the conditions are to be determined, and so on. Since there is a lack of sufficient guidance, this provision is also subject to misuse.

While there are other provisions where the government has powers to prescribe conditions and make substantive rules, the examples highlighted above provide almost no guidance. This is also problematic when judged against the tenets of Indian administrative law, which requires that laws should not confer unguided and excessive discretion on the implementing authority.[28] If improperly used, such legal provisions are potentially in violation of the Indian Constitution.

Third, the design of the DPB is problematic. The board is an independent agency with a limited mandate, and the government will create mechanisms for the selection and appointment of its members. While the law sets out qualifications for members, it does not state how many members shall be on the board and requires only one of them to be a legal expert. This last provision is a problem since one of the board's main functions is to issue penalties and directions for noncompliance.

In addition, the chairperson of the DPB is empowered to authorize any board member to perform "any of the functions of the board and conduct any of its proceedings." It is possible that the chairperson may not authorize the legal member of the board to conduct the proceedings leading up to the issuance of a penalty. This design also fails to maintain an internal separation of functions between the members conducting inquiries and the chairperson. Since the chairperson appoints members to conduct inquiries, they may potentially not discharge this function impartially in all cases.

Therefore, while the DPDP Act creates data privacy protections in law for the first time, certain provisions in the law can effectively undermine its benefits if the government does not act under them in the most scrupulous manner possible.

Tracing the Evolution of the Debate on the Legislation

The DPDP Act is a remarkable shift in the approach toward data protection legislation compared to the 2018 draft bill and the 2019 bill introduced in Parliament. This shift was most visible in the November 2022 draft bill and has now been enshrined in the 2023 law. There are three major axes on which this shift is visible.

1. Reductions in rights and obligations, and compliance: The 2018 and 2019 versions of the bill adopted a more expansive and all-encompassing framework toward data protection. As the preceding sections of this paper explain, many of these rights and obligations have been either diluted or discarded—data portability, for example, has been completely removed, while others such as the right to be forgotten have been recast to a simpler right to "erasure."

   Detailed prescriptions regarding the contents of notices and privacy by design requirements, among others, have been discarded, and it is now up to businesses to translate these requirements. This is a better and more innovation-friendly approach. Given the lack of prior data protection law and jurisprudence, firms will experiment with different approaches to translate them into business practices. The practices that do not meet the requirements of the DPDP Act will be adjudicated in the DPB, the TDSAT, and the courts. This process will provide for an organic emergence of good practices suited to the Indian context.

   This reduction in prescriptive requirements and overall compliance should also be seen in the context of the shift away from criminalization. The 2018 bill created a number of criminal offenses. The 2019 bill reduced this to just one—deanonymization. The 2022 draft and the 2023 version do not provide for any criminal offenses and stipulate only monetary penalties to be directed by the DPB.

2. A sharper focus on data privacy: The 2018 draft, and more so the 2019 draft, included several provisions that were only tangentially related to data privacy. For example, the provision mandating the sharing of nonpersonal data did not further privacy interests in any way. Similarly, data localization requirements have been shown to have only a tangential relationship to data privacy, and better alternatives exist to achieve the same objectives. Their presence in the 2018 and 2019 bills were a source of uncertainty. In addition, data localization became a proxy for debates on issues such as data sovereignty, something that, again, is not directly related to the issue of privacy.

3. The abandonment of a "regulatory" law: The 2018 and 2019 bills created a legislative framework that had a high degree of regulatory intensity—the bills provided a full-fledged independent regulator, the DPA, with extensive powers to frame regulations and codes of conduct on many provisions within those bills, such as notice and consent requirements, security safeguards, manner of storage of data, and so on. In addition, the DPA would have had powers to collect information necessary for ensuring compliance with the law and impose penalties for noncompliance. The DPA, therefore, was proposed to have many more touchpoints with the economy, and its mandate, by definition, required it to be relatively more interventionist.

   These legislative proposals made the DPA a centerpiece of the regulatory framework, and the agency was expected to function like other Indian independent regulators,

such as the Securities and Exchange Board of India and the Telecom Regulatory Authority of India. The DPA was expected to exercise these powers across all sectors of the Indian economy. It would have had to prescribe standards for all the legal provisions that provided for standard-setting requirements through regulations, modify and update them periodically, conduct the necessary stakeholder consultations across different economic sectors, create or identify research to support its regulatory agenda, and build its regulatory legitimacy. The proposed legislative role of the DPA in 2018 and 2019 was thus one of high regulatory intensity. Given this wide remit, it would have faced obvious challenges related to deciding on its overall approach, prioritizing among its many functions and objectives, and building the internal capabilities required to deliver on this expansive mandate.

The DPDP Act does away with the idea of an independent regulator like the DPA. The DPB does not have many regulation-making powers under this law. Its powers are limited to ensuring remedial actions against any data breaches and issuing directions to businesses requiring them to comply with the law. In addition, the DPB can pass orders issuing penalties or imposing voluntary settlements for noncompliance with the law. This is not a design that is "regulatory" in the same way as the proposed DPA in the 2018 and 2019 versions and is a major shift in approach. The DPB's limited mandate will create less frequent touchpoints with the economy even though its orders regarding compliance or noncompliance will be extremely consequential.

These shifts have occurred incrementally over the last few years. The 2018 bill proposed an expansive law based closely on the GDPR. The 2019 bill rationalized some provisions while retaining most of them and adding to the regulatory expanse. It imported concerns that were at best tangential to privacy concerns in some cases. The 2022 bill and the 2023 act are a major shift away from this expansive framework. This indicates a change in how Parliament and the Indian government now view the salience of the data protection law to India's economy. In 2017 and 2018, there were a few animating factors that led to the early versions of the bill. The Supreme Court had recently declared privacy to be a fundamental right and was about to rule on the constitutionality of India's biometric ID project, Aadhaar. In addition, there was a global debate on data protection regulation sparked off by the impending implementation of the GDPR. The regulation was enacted in 2016 and came into force in 2018. At that point in time, it was viewed as a viable template for adoption and influenced deliberations on the Indian law.[29]

By 2022, the GDPR had been in effect for four years, and numerous issues with its design and implementation had been voiced.[30] The Indian Supreme Court had upheld the use of Aadhaar for certain purposes and the potential constitutional law issues had been resolved. Arguably, deliberations on the different versions of the data protection legislation also allowed concerns about the proposed framework to be articulated consistently. This was especially visible on issues such as data localization.[31] The long period of deliberations, therefore, allowed the shift to a more pragmatic version of the law to be finally enacted.

However, one part of the government's approach toward the law has remained noticeably consistent—the exemptions given for state functions. State surveillance agencies have been consistently exempted from the application of data protection requirements. The 2018 draft bill sought to narrow the scope of exemptions and proposed some checks and balances, which were diluted in the 2019 bill. The 2019 bill instead gave the central government the power to exempt any national security agency from any or all provisions of the proposed legislation. A similar provision has now been enacted into the law—other non-security-related government uses of data will continue to be exempted from certain parts of the law. Lastly, as pointed out earlier, the DPDP Act also gives the government problematic levels of unfettered discretion in some cases.

The next part of this paper speculates on how two developing strains of data-related regulation—the working of the data protection law and the concerns of national security and sovereignty—are likely to inform the next stage of data regulation in India.

Looking Forward to the Implementation of the Data Protection Law

Now that the DPDP Act is law, there will be three key sources of regulatory development under the same.

The first will be the rules framed by the central government to implement the law. The DPDP Act provides significant rule-making powers to the central government. These include:

- the manner in which notices will be given to consumers;[32]
- the manner in which consent managers will function;[33]
- the manner in which businesses will inform their consumers and the DPB about data breaches;[34]
- the manner in which parental consent will be sought for processing children's data and related exemptions;[35]
- the manner in which consumers will exercise their rights against data fiduciaries;[36]
- the manner of appointment of DPB members, the terms and conditions of their service, and the procedures for the functioning of the board;[37]

- data impact assessments and other measures to be taken by significant data fiduciaries;[38] and

- the procedure to be followed by the appellate tribunal, the TDSAT, in hearing appeals from the DPB.[39]

These are not insignificant powers. However, as already discussed, these powers of rule-making pale in comparison to the ones that were proposed to be given to the DPA under the previously proposed versions of the law. The intensity of regulation will, therefore, be much lower under the DPDP Act than it would have been under the 2019 bill. In creating this framework, the Indian Parliament has opted for a modest approach to creating elaborate rules and regulations. This will consequentially allow greater scope for experimentation and innovation in the Indian technology landscape relative to the 2019 bill and its predecessor.

While many of these powers pertain to procedural issues, the central government has substantive rule-making powers as well. The fact that these rule-making powers are with the central government is problematic.

The most consequential of these is the power to grant exemptions. The exercise of this power will be contingent on two factors—the degree of technocratic competency within the relevant departments of the central government and the degree to which the relevant officers can function autonomously and technocratically. Historically, the Indian state's response to improve competence and autonomy in economic regulation has been to move these functions to independent regulatory agencies. In this case, however, such powers have been retained with the central government.

On the other hand, the lack of any prior regulatory expertise on data protection also lends itself to an argument in favor of greater political inputs at an incipient stage of regulatory development. Historically, the Indian government directly regulated many subjects before transferring them to independent regulators and, in the process, developed a certain degree of institutional capability within the relevant departments. This has been the case for various subjects such as insurance, pension, telecom, electricity, and so on. While these departments did not necessarily regulate well, the exercise of these powers did create some technical and supervisory capacity within the relevant departments.

The critical consideration, therefore, is whether the drafters of the DPDP Act consider the framework under the law as a first step in the development of an independent regulator.

The second key source of regulatory development will be the decisions of the DPB in cases where it initiates an inquiry against regulated entities. The reasoning of the DPB and the penalties and directions it issues will be the first set of decisions on data privacy regulation under a new law. These decisions will not just contribute to jurisprudence on the subject but also provide guidance to businesses on how to implement and comply with the DPDP Act. The procedures the board follows, the quality of its reasoning, and the clarity of its decisions will shape both market behavior and future regulation in India.

In this regard, the composition of the board and the qualifications of its members conducting inquiries will be critical. The law has definite weaknesses in this regard, as discussed earlier. The proper implementation of the law will, therefore, depend on the government adopting best practices in appointment and selection and creating a culture of noninterference, since the law does not contain many standard provisions present in other Indian laws.

The third key source of regulatory development will be the directions that the DPB is empowered to issue under the law. While the DPDP Act requires the board to observe certain specified procedural rules while conducting inquiries and issuing penalties, it does not provide any such guidance for issuing directions to regulated entities. This is problematic since directions will also be binding and impose compliance costs. It is, therefore, appropriate that the board should create certain checks and balances for issuing directions. At the very least, the board should provide any regulated entity with a formal opportunity to furnish their response to a draft direction before such a direction is formally issued to them. Absent this, the board may develop a predilection toward regulation by direction.

The trajectory of these three strands of regulatory decision-making will significantly shape India's technology markets and data-related policy for the next few years. Since the law does not contain adequate checks and balances, the onus will be on the central government to ensure that best practices in administrative law and decisionmaking are incorporated via the procedural rules that the DPDP Act empowers it to make.

The other main factor that will shape the development of data protection regulation will be the larger imperatives of exercising sovereign control over data and data businesses in India. The development of the DPDP Act was significantly influenced by the call to exercise control over Indian data for the benefit of Indians. This was most visible during the debate on issues related to data localization and nonpersonal data. While the provisions in the final law represent a significant moderation from the provisions in the draft proposals, the larger concerns over sovereignty and security will influence the development of this law.

One clear example of this is Section 37 of the law that enables the central government to block access to any information that can be communicated by a data fiduciary. This is a new insertion, and it is highly debatable whether this provision has any relevance to personal data privacy.

Outside the DPDP Act, the evolving framework of laws regulating social media companies, IT services, and businesses, among others, will also exercise indirect influence on how data protection regulation develops. In 2021, the Indian government issued new guidelines for social media intermediaries that required, among others, measures to trace originators of social media content on over-the-top (OTT) messaging platforms. These requirements were challenged in courts and a final decision is awaited. The outcome will determine the nature and scope of the powers enjoyed by investigative agencies under the exemptions granted by the DPDP Act.

Another example is that of data localization. While the DPDP Act does not restrict data flows across borders, many Indian sectoral regulators, like the Reserve Bank of India, do impose localization requirements. The progressive adoption of localization by other regulators may make the liberal provisions of the DPDP Act superfluous.

Some legal requirements aimed at regulating social media and big tech companies are emanating organically due to India's rapid digital transformation in the past decade and the fact that the regulatory framework is outdated.[40] India's IT minister has stated that a replacement to India's Information Technology Act, 2000 is in the works. This newer version of the IT Act, as well as other similar legislations, is also likely to influence the working of the DPDP Act. In each of these developments, it will be important to ensure that the nature and scope of sovereign control to be exercised is for a legitimate purpose and that it does not overserve the needs of the Indian state to the detriment of privacy, commerce, and innovation.

Conclusion

While the DPDP Act is a culmination of more than five years of debate and deliberation, it marks the start of statutory personal data protection regulation. The regulatory developments and the institutional arrangements that take shape over the next few years will decide how well (or not) personal data privacy is protected. The new law provides the necessary scaffolding, but it is not sufficient for de facto data privacy to materialize.

It is debatable whether the earlier versions of the bill would have resulted in better privacy protection in any meaningful way.[41] However, the transformation of the contents of different versions of the law is indicative of the changed approach of the government to privacy protection. The fact that the current version of the law, as compared to the earlier ones, imposes much lower costs on Indian businesses is positive.

Overall, the law itself is modest and pragmatic. This is welcome. However, in some cases, it is exceedingly so, to the potential detriment of privacy interests. The fact that a significant degree of discretionary power on substantive issues is vested with the central government means that a lot will depend on how well the government is committed to protecting privacy.

About the Author

Anirudh Burman is an associate research director and fellow at Carnegie India. He works on key issues relating to public institutions, public administration, the administrative and regulatory state, and state capacity. He has also worked extensively on financial regulation and regulatory governance.

Notes

1 The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), *Gazette of India*, August 11, 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

2 Starting with the Supreme Court's judgment declaring privacy to be a fundamental right in *Justice K.S. Puttaswamy and Anr. v. Union of India and Ors*. (10 SCC 1, Supreme Court of India, 2017).

3 The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019), accessed December 16, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

4 The Personal Data Protection Bill, 2018, accessed March 8, 2019, https://www.thehinducentre.com/resources/article24561526.ece/binary/Personal_Data_Protection_Bill,2018_0.

5 "Report of the Joint Committee on the Personal Data Protection Bill, 2019," 17th Lok Sabha Secretariat, December 16, 2021, https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

6 The Digital Personal Data Protection Bill, 2022, Ministry of Electronics & Information Technology, Government of India, accessed August 9, 2023, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.

7 *Justice K.S. Puttaswamy and Anr. v. Union of India and Ors*.

8 Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?," Carnegie India, March 9, 2020, https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217.

9 Ibid.

10 "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union*, May 4, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

11 Anirudh Burman, "The Withdrawal of the Proposed Data Protection Law Is a Pragmatic Move," Carnegie India, August 22, 2022, https://carnegieindia.org/2022/08/22/withdrawal-of-proposed-data-protection-law-is-pragmatic-move-pub-87710.

12 The Digital Personal Data Protection Bill, 2022.

13 Ibid., Section 3.

14 The Digital Personal Data Protection Act, 2023, Section 4.

15 Ibid., Section 7(b).

16 Ibid., Section 7.

17 See ibid., Sections 11–14.

18 Ibid., Sections 8 and 9.

19 Ibid., Section 10.

20 Ibid., Section 17(1).

21 Ibid., Section 17(2).

22 Ibid., Section 18.

23 Ibid., Sections 27 and 28.

24 Ibid., Sections 19 and 20.

25 Ibid., Schedule to the Act, Section 33.

26 Ibid., Section 32.

27 Ibid., Section 17(1)(c).

28 See, for example, *A.N. Parasuraman etc. v. State of Tamil Nadu* [SCC (4) 683, 4 Supreme Court Cases 683, Supreme Court of India, 1989]; *Agricultural Market Committee v. Shalimar Chemical Works Ltd.* [Supp. (1) SCR 164, Supp. (1) Supreme Court Reporter 164, Supreme Court of India, 1997]. In this case, the court observed that "the essential legislative function consists of the determination of the legislative policy and the Legislature cannot abdicate essential legislative function in favour of another. . . . The Legislature should, before delegating, enunciate either expressly or by implication, the policy and the principles for the guidance of the delegates." See also I.P. Massey, "Chapter 4" in *Administrative Law*, 10th ed. (Lucknow: Eastern Book Company, 2022), 94–104.

29 See, for example, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Ministry of Electronics & Information Technology, Government of India, July 27, 2018, 3, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf: "The EU, at the vanguard of global data protection norms has recently enacted the EU GDPR, which has come into force on 25 May 2018. . . . It is a comprehensive legal framework. . . . It is both technology and sector-agnostic and lays down the fundamental norms to protect the privacy of Europeans. . . . We are informed that 67 out of 120 countries outside Europe largely adopt this framework or that of its predecessor."

30 See, for example, Axel Voss, "Fixing the GDPR: Towards Version 2.0," EPP Group in the European Parliament, May 25, 2021, https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf; Daniel Mikkelsen et al., "GDPR compliance since May 2018: A continuing challenge," McKinsey & Company, July 22, 2019, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge; Martin Brinnen and Daniel Westman, *What's wrong with the GDPR? Description of the challenges for business and some proposals for improvement*, Svenskt Naringsliv - Swedish Enterprise, December 2019, https://www.svensktnaringsliv.se/material/skrivelser/xf8sub_whats-wrong-with-the-gdpr-webbpdf_1005076.html/What%27s+wrong+with+the+GDPR+Webb.pdf; Ilse Heine, "3 Years Later: An Analysis of GDPR Enforcement," *Strategic Technologies Blog*, Center for Strategic & International Studies, September 13, 2021, https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement; Alec Stapp, "Against Privacy Fundamentalism in the United States," Niskanen Center, November 19, 2018, https://www.niskanencenter.org/against-privacy-fundamentalism-in-the-united-states/.

31 Soumyarendra Barik, "For better compliance, tech transfer, Govt to ease data localisation norms," *Indian Express*, August 14, 2022, https://indianexpress.com/article/india/for-better-compliance-tech-transfer-govt-to-ease-data-localisation-norms-8088627/.

32 The Digital Personal Data Protection Act, 2023, Section 5.

33 Ibid., Section 6(8).

34 Ibid., Section 8(6).

35 Ibid., Section 9.

36 Ibid., Sections 11, 12, 13, and 14.

37 Ibid., Sections 22, 23, and 28.

38 Ibid., Section 10(2).

39 Ibid., Section 29(8).

40 For more on this, see the section on data in Suyash Rai and Anirudh Burman, "India: Testing Out New Policies on Globalization - Rewiring Globalization," in *Rewiring Globalization,* Sinan Ülgen et al. (Brussels: Carnegie Europe, 2022), https://carnegieindia.org/2022/02/17/india-testing-out-new-policies-on-globalization-pub-86370.

41 Burman, "Will India's Proposed Data Protection Law."

Carnegie India

Founded in 2016, Carnegie India, based in New Delhi, is part of a robust global network that includes over 150 scholars in more than twenty countries around the world. The center focuses primarily on three interrelated programs: technology and society, political economy, and security studies. Led by Indian experts with decades of international and domestic policy experience, Carnegie India engages with governments, policymakers, academics, students, industries, practitioners, and civil society to provide insightful and fresh analysis on India's pressing challenges and the rising role of India in the world.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

CARNEGIE
INDIA

CarnegieIndia.org