Non-final version of Parsheera; Smriti. Awaiting the dawn of data protection regulation in India; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

AWAITING THE DAWN OF DATA PROTECTION REGULATION IN INDIA

Smriti Parsheera

Abstract

This chapter traces the history of India's journey in formulating a data protection law. Policy thinking on this issue was under progress for well over a decade and finally translated into a legislative outcome through the Digital Personal Data Protection Act, 2023. This law signals the dawn of a new phase in India's digital journey. While it is a necessary start, the contents of India's new law still leave much to be desired. The chapter highlights some key issues like the weakened scope of protections compared to global examples and previous drafts of India's bills and the broad scope of exemptions for government agencies in the law. As the consequences of these limitations come to light, the law will likely have to evolve further through legislative or judicial interventions. In parallel, there is also much to be done in terms of institution building and rule-making to give life to the new law.

Non-final version of Parsheera; Smriti. Awaiting the dawn of data protection regulation in India; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CONTENTS

Awaiting the dawn of data protection regulation in India 1

1. Awaiting the dawn of data protection regulation in India 1

1.1. Introduction 1

1.2. Decade of legislative attempts 3

1.3. Data protection under existing instruments 5

1.4. Overview and analysis of the DPD Act, 2023 7

1.4.1. Diminished rights and protections 10

1.4.2. Exemptions for state agencies 11

1.4.3. Impact on right to information 12

1.4.4. Concerns with the regulatory structure 13

1.4.5. Cross border data flows 14

1.5. Other developments: Architectures and proposals on data governance 15

1.6. Automated Personal Data Processing 16

1.7. Conclusion 17

2. Annex: The Digital Personal Data Protection Act 21

Non-final version of Parsheera; Smriti. Awaiting the dawn of data protection regulation in India; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

1. AWAITING THE DAWN OF DATA PROTECTION REGULATION IN INDIA

1.1. Introduction

India is one of the world's most rapidly growing digital markets. It houses the world's second largest Internet user base, is a well-known hub of information technology services, and has a vibrant digital market characterised by the coexistence of global technology players and domestic businesses. The Indian government has, in tandem, been working towards building a more digitally connected society through initiatives such as the biometric digital identity project, Aadhaar, improved broadband connectivity, digital payments and e-governance reforms. It has also been promoting a home-grown model of digital public infrastructure development under the 'India Stack' brand. India Stack refers to a collection of state-backed digital interventions designed to promote interoperability among public and private actors in areas like digital identity, digital payments, digital records management, and personal data sharing.[1] This is reflective of the broader trend towards promoting technological autonomy and local innovation as a pathway to national development, which can be observed among other BRICS nations as well.[2]

Several of the developments pointed to above, across the public and private sectors, ride upon the collection, processing and sharing of the personal data of individuals. Yet, despite the prevalence of so many data-centric activities, until very recently, India did not have a comprehensive data protection law to govern such practices. This situation is now expected to change pursuant to India's adoption of the *Digital Personal Data Protection Act, 2023* (DPD Act) on 11 August, 2023.[3] However, this law is yet to be brought into effect. Until that happens, individuals continue to remain only partially protected by a patchwork of laws and directives, leaving them vulnerable to the widespread collection, processing and misuse of personal data.

The Indian experience stands out from the other BRICS nations both in term of its stage of adoption of the data protection law — the other four countries in the original BRICS grouping already have a functional data protection framework — and the scope and terminology that it adopts. Unlike most other data protection laws that cover personal data in all its forms (digital and physical), the DPD Act is saor was digitised after being collected through other means.[4] It defines the persons who determine the purpose and means of processing of personal data as 'data fiduciaries', a term that is meant to signify the high level of responsibility that they must bear towards the individual. However, as the discussions that follow will reveal, this does not necessarily translate to offering a higher standard of protections being offered by the law. In addition to the obligations of data fiduciaries, the DPD Act sets out the rights and duties of data principals, which is the term used to refer to individuals whose personal data is being protected. Further, the DPD Act lays the foundation for the establishment of a new agency, called the Data Protection Board of India (DP Board). This body is yet to be constituted by the Indian government. Some preliminary steps in that direction were initiated recently with the release of the Draft Digital Personal Data Protection Rules, 2025 (Draft Rules) that were published in January, 2025 and we open

---

[1] Smriti Parsheera, 'Stack is the New Black: Evolution and Outcomes of the 'India-Stackification' Process' 52 Computer Law & Security Review (April 2024) <https://doi.org/10.1016/j.clsr.2024.105947> accessed 1 April 2025.

[2] Luca Belli and Larissa Galdino de Magalhaes, 'Editorial: Toward a BRICS stack? Leveraging digital transformation to construct digital sovereignty in the BRICS countries' 55 Computer Law & Security Review (November 2024) < https://doi.org/10.1016/j.clsr.2024.106064 > accessed 1 April 2025.

[3] Digital Personal Data Protection Act, 2023 <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf> accessed 21 August 2023.

[4] DPD Act, 2023, s 3(a).

for public comments till the beginning March.[5] Among other things, the Draft Rules outline the process for appointment of the DP Board's chair and members and their terms of service.

The enactment of the DPD Act follows a series of events and discussions that have been going on for well over a decade. One of these events was the 2017 landmark decision by the Indian Supreme Court affirming that privacy constitutes a fundamental right under the Indian Constitution.[6] In the years that followed five different versions of a data protection bill were put out in the public domain. This process began with the setting up of a committee of experts chaired by former Supreme Court judge, Justice B.N. Srikrishna, in 2018 that recommended a draft data protection bill for the consideration of the government.[7] Following this, the Indian government introduced a bill titled the Personal Data Protection Bill, 2019 (PDP Bill, 2019) in the Parliament signalling a clear legislative intent to regulate this area.[8] The 2019 bill went through several rounds of public consultation, including in the course of its review by a Joint Parliamentary Committee. However, despite these efforts, in August 2022, the Ministry of Information Technology and Electronics (MeitY), the ministry in-charge of the subject, unexpectedly announced the government's decision to withdraw the PDP Bill, 2019.[9]

The MeitY then put out a new draft called the Digital Personal Data Protection Bill, 2022 (DPD Bill, 2022) for public comments in December, 2022.[10] In a move that deterred an open and transparent debate, the government announced that the submissions received on this draft would not be disclosed publicly.[11] In the months that followed, the MeitY reworked this version of the draft bill and introduced the Digital Personal Data Protection Bill, 2023 in the Lok Sabha, the lower house of the Indian Parliament, on 3rd August, 2023.[12] Just four days after its introduction, the bill was passed by the Lok Sabha and subsequently by the Rajya Sabha, the upper house of the Indian Parliament, on 9th August. The Bill then received the President's assent and was notified as the DPD Act on 11th August. While India is not alone in terms of its long drawn process of developing a data protection law the lack of consistency and clarity of direction in the effort is worth noting. For example, the negotiation of the Brazilian data protection also spanned across a similar duration but with relatively better coherence between the different stages of the process.

Set against the background of these developments, this chapter offers a brief history of India's journey in formulating its data protection law. It focuses, in particular, on the latest phase of this process involving the introduction and adoption of the DPD Act, 2023. As the discussions in this chapter will reveal, the DPD Act is substantially different from the earlier bills that came out in 2018 and 2019, and had been under

---

[5] Draft Digital Personal Data Protection Rules, 2025 <https://static.mygov.in/innovateindia/2025/01/03/mygov-999999999568142946.pdf> accessed 1 April 2025.

[6] *Justice K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1.

[7] B.N. Srikrishna et al., 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians' (Ministry of Information Technology and Electronics, July, 2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 19 April 2023.

[8] Personal Data Protection Bill (PDP Bill), 2019 (Lok Sabha, 2019) <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf> accessed 19 April 2023.

[9] 'Union government rolls back Data Protection Bill' (The Hindu, 3 August 2022) <https://www.thehindu.com/news/national/union-government-rolls-back-data-protection-bill/article65721160.ece> accessed 19 April 2023.

[10] Draft Digital Personal Data Protection Bill, 2022 (Ministry of Electronics & Information Technology, December 2022) <https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf> accessed 19 April 2023.

[11] Ministry of Electronics & Information Technology, 'MeitY invites feedback on the draft "Digital Personal Data Protection Bill 2022"' (Press Information Bureau, 18 November 2023) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1877030> accessed 19 April 2023.

[12] Digital Personal Data Protection Bill, 2023, Bill No. 113 of 2023, <https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/113_2023_LS_Eng83202330313PM.pdf?source=legislation>

discussion for about half a decade. The chapter describes the context in which the proposals for a legislation evolved over the years and the significant ways in which it differs from the versions that preceded it. While doing so it highlights some of the key substantive provisions of the DPD Act as well as issues that remain with it. It identifies the limited scope of rights and protections offered by the 2023 Act, broad brushed exemptions and a diluted regulatory structure as some areas of concern.

The discussions that follow would benefit from a brief overview of the legal system and rule of law context in the country. India is a parliamentary democracy with legislative functions divided between the union and state governments. At the union level, the Constitution of India allows a legislative proposal in the form of a bill to be introduced in either house of the Parliament. These houses are the Lok Sabha, consisting of members elected through direct elections, and the Rajya Sabha, consisting of representatives of various Indian States and nominated members.[13] The bill then needs to be approved by both the houses and receive the President's assent following which it is notified as a law.[14] The Constitution also guarantees a spectrum of fundamental rights and provides for the judicial review of legislative and administrative actions that may infringe upon those rights.

In 2023, the Freedom in the World report, which assesses the level of political rights and civil liberties across jurisdictions, classified India under the 'partly free' category.[15] The report observed that although India's Constitution guarantees various civil liberties, there had been instances of harassment of nongovernmental organizations and government critics, which diminished these freedoms in practice. The Freedom on the Net report produced by the same organisation similarly gave India a partly free rating with score of 13/25 for obstacles to access, 20/35 for limits on content and 17/40 for violations of user rights.[16] Another study by a United Kingdom based website called Comparitech examined the state of surveillance in 47 countries and found India to be the third worst performer, classifying it as having 'systemic failure to maintain safeguards'.[17] However, to put this in context, the study did not find any of the examined countries to be upholding privacy standards on a consistent basis nor as having significant safeguards and protections. Further, India's assessment was conducted prior to the enactment of the DPD Act, which may lead to some improvement in its performance going forward.

1.2. Decade of legislative attempts

Prior to the enactment of the DPD Act, the debate around the introduction of data protection legislation in India had been under progress for over a decade. Much of this was closely intertwined with the developments around the government's digital identity program, Aadhaar. The Aadhaar project, which now covers over 1.4 billion individuals, was designed to provide a verifiable, unique and foundational digital ID to all of India's residents. The project relies on the collection of biometric and demographic data of individuals as the basis for the issuance of digital identities to them and the subsequent use of this information for authentication purposes. Aadhaar was launched in 2009 through an executive order and without any legislative backing. A Parliamentary Standing Committee that reviewed a proposed bill on the subject observed that the adoption of a data protection law had to be a prerequisite for the unique biometric identity project.[18] Alongside the Aadhaar project, the interaction between privacy and

[13] Rajya Sabha Secretariat, 'The Law Making Process' (Parliament of India, 2020) <https://rajyasabha.nic.in/rsnew/information_booklet/Law_Making.pdf> accessed 19 April, 2023.

[14] The process differs for Money Bills on which the Lok Sabha enjoys exclusive legislative powers and the Rajya Sabha only exercises recommendatory functions.

[15] Freedom in the World, 2023 (Freedom House, 2023) <https://freedomhouse.org/country/india/freedom-world/2023#PR> accessed 29 November 2023.

[16] Freedom on the Net, 2023 (Freedom House, 2023) <https://freedomhouse.org/country/india/freedom-net/2023> accessed 29 November 2023.

[17] Paul Bischoff, Data privacy laws & government surveillance by country: Which countries best protect their citizens? (Comparitech, 26 March 2022) <https://www.comparitech.com/blog/vpn-privacy/surveillance-states/> accessed 29 November 2023.

[18] Department-related Parliamentary Standing Committee on Finance, 'Forty-Second Report on National Identification Authority of India Bill, 2010' (Lok Sabha Secretariat, 2011) 33

disclosure requirements under the country's public transparency law called the Right to Information (RTI) Act, 2005 also fed into the need for a discussion on privacy regulation.[19] This need was intensified by the announcement of the National Intelligence Grid (NATGRID) project, which was meant to facilitate information sharing between domestic intelligence agencies for counter-terrorism measures, sparking concerns of a centralised surveillance apparatus being built by the government.

All of these factors served as an impetus for the government to set up a Group of Experts on Privacy in 2011. The expert group was asked to make suggestions for a proposed draft bill on privacy.[20] This was to be informed by a review of similar laws adopted by other countries and an analysis of the privacy impact of various government programmes in India. In its recommendations submitted to the government in October 2012, the expert group suggested nine principles and five salient features of the data privacy framework for India.[21] These features were, technological neutrality and interoperability with international standards, a multi-dimensional understanding of privacy, horizontal applicability, conformity with privacy principles, and a co-regulatory enforcement regime. However, these recommendations and efforts at the formulation of a draft data privacy bill did not translate into legislative action although several 'leaked' versions of a draft bill emerged between 2011 to 2014.[22]

While the process of formulating a law on data privacy effectively came to a standstill, the Aadhaar project was scaled up and continued to function for several years without the backing of a statutory framework. The sensitive nature of Aadhaar data and its extensive adoption in the public and private spheres, in many cases on a mandatory basis, led to challenges being filed before courts questioning the constitutional validity of Aadhaar. In the context of these challenges, the Indian Supreme Court constituted a nine-judge bench to look into the question of whether privacy can be regarded as a fundamental right under the Indian constitution.[23] In what is popularly referred to as the *Puttaswamy* privacy verdict, the judges of the Supreme Court unanimously answered this in the affirmative. By doing so, this judgement laid the groundwork for the subsequent verification of Aadhaar's compliance with the fundamental right to privacy by a different bench of the Supreme Court.[24]

The *Puttaswamy* privacy verdict emphasised that privacy has both positive and negative dimensions. On behalf of four of the judges, Justice Chandrachud noted that, "*the negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual*".[25] The judges then went on to highlight the need for a robust regime for data protection that would strike a careful balance between individual interests and legitimate concerns of the state. In a bid to demonstrate this positive commitment towards privacy, the MeitY constituted the Justice B.N. Srikrishna-led committee of experts on data protection while hearings were still going on in the *Puttaswamy* privacy case. This nine-

<https://uidai.gov.in/images/report_of_the_departmental_standing_committee_on_finance_on_the_bill_13012017.pdf> accessed 19 April 2023.

[19] The creation of NATGRID was announced in 2009 as a response to the terrorist attacks in Mumbai but the project has seen a series of delays until the recent opening of a new NATGRID campus in the city of Bengaluru in May, 2022. See Amit Chaturvedi, 'Delayed by Covid, NATGRID likely to be implemented soon' (Hindustan Times, 14 September 2021) <https://www.hindustantimes.com/india-news/delayed-by-covid-natgrid-likely-to-be-implemented-soon-check-details-101631609979429.html> accessed 19 April 2023; Ministry of Home Affairs, 'The Union Minister for Home and Cooperation, Shri Amit Shah inaugurated the National Intelligence Grid (NATGRID) Bengaluru campus today', (Press Information Bureau, 3 May 2022) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1822356> accessed 19 April 2023.

[20] Planning Commission, Government of India, Group of Experts on Privacy Submit Report'(Press Information Bureau, 18 October 2012) <https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503> accessed 19 April 2023.

[21] A.P. Shah et al, 'Report of the Group of Experts on Privacy' (Planning Commission, 2012) <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf> accessed 19 April 2019.

[22] Malavika Raghavan, 'Are we there yet?: The long road to nowhere, the demise of India's data protection bill' (Future of Privacy Forum, 11 October 2022) <https://fpf.org/blog/are-we-there-yet-the-long-road-to-nowhere-the-demise-of-indias-draft-data-protection-bill/> accessed 19 April 2019.

[23] *Justice K.S. Puttaswamy* v. *Union of India* (n 7).

[24] *Justice K.S. Puttaswamy* v. *Union of India*, (2019) 1 SCC 1.

[25] *Justice K.S. Puttaswamy* v. *Union of India* (n 7), part T, para 3(I).

member Committee was requested to study issues relating to data protection in India and make suggestions on the key principles along with the formulation of a draft data protection bill.

The committee submitted a report titled "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" to the government in July, 2018.[26] This was accompanied by a draft of the proposed PDP Bill, 2018[27] that led to the introduction of the PDP Bill, 2019 in Parliament in December, 2019.[28] This bill was referred to a 30 member Joint Parliamentary Committee (JPC) consisting of representatives from both the houses of the Parliament. Following a two-year long process of internal deliberations, written comments from the public, and selective in-person hearings, the JPC submitted its report along with a revised draft of the 2019 bill.[29]

However, soon after that the Union Minister of MeitY announced that the government had decided to withdraw the PDP Bill, 2019. The explanation given was that since the JPC had suggested several changes to the 2019 bill, the Ministry was in the process of developing a revised and comprehensive draft law.[30] Aside from the officially stated reason it is known that the previous bill saw significant resistance from the private sector on the grounds of the compliance costs that would be imposed upon them. Reports suggested that the US tech industry had also approached Indian government agencies with a proposal to form a new working group to discuss issues with the previous bill.[31]

These pressures are likely to have played a role in shaping the DPD Act, with some describing the 2022 draft bill as a 'more tech friendly data protection bill'.[32] Section 4 of this chapter demonstrates some of the ways in which the DPD Act presents a significantly stripped-down version of the previous legislative proposals. This is reflected in the dilution of the compliance obligations imposed on the industry, widened government exemptions and a weakened regulatory structure for the implementation of the law.

1.3. Data protection under existing instruments

Pending the adoption of a comprehensive law on data protection, limited protections for safeguarding personal data were available under the Information Technology Act, 2000 (IT Act), the rules framed under it, and certain sectoral laws.[33] The IT Act contains only two sections engaging with the subject of data privacy – Sections 43A and 72A – both of which were inserted through an amendment to the law in 2008. Section 43A of the IT Act imposes an obligation to pay compensation on a body corporate that fails to maintain reasonable security practices in respect of sensitive personal data resulting in a wrongful gain or loss to an individual. Upon the implementation of the DPD Act, this section will be omitted from the IT Act.[34] Section 72A, the other relevant provision in the IT Act, is a penalty provision that imposes a

[26] B.N. Srikrishna et al., A Free and Fair Digital Economy Protecting Privacy (n 8).
[27] The (Draft) Personal Data Protection Bill, 2018 (Ministry of Electronics and InformationTechnology, 2018) <https://www.meity.gov.in/writereaddata/files/Personal Data Protection Bill, 2018.pdf> accessed 19 April, 2023.
[28] PDP Bill, 2019 (n 9).
[29] P.P. Chaudhary et al. 'Report of the Joint Committee on Personal Data Protection Bill, 2019' (Lok Sabha Secretariat, 2021) <http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/pr_files/Press%20Release%20on%20the%20presentation%20Report.pdf> accessed 19 April 2023.
[30] The Hindu, 'Union government rolls back Data Protection Bill' (n 10).
[31] Soumyarendra Barik and Aashish Aryan, 'US bodies push back on data protection Bill, seek new working group' (The Indian Express, 3 March 2022) <https://indianexpress.com/article/india/us-bodies-push-back-on-data-protection-bill-seek-new-working-group-7798193/> accessed 1 April 2025.
[32] John Reed, India releases more tech friendly data protection bill after backlash, Financial Times, November 21 2022 <https://www.ft.com/content/0a72f522-2bfe-4da5-a831-2c96c8ce52ff> accessed 19 April 2023.
[33] Information Technology Act, 2000 <https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf> accessed 19 April 2023; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 <https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf> accessed 19 April 2023.
[34] DPD Act, s 44(2)(a).

punishment for unauthorised disclosure of personal information obtained under a contract. It lays down a punishment in the form of imprisonment of up to three years and/or a fine up to five hundred thousand rupees.

In addition to these statutory provisions, the government has notified a set of rules on the protection of sensitive personal data under Section 43A known as the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules). The IT Rules reflect several of the safeguards that are typically seen in data protection laws, such as requirements of notice and consent, permission for disclosure, and limitations on cross border transfers. While on paper this may have seemed like a passable framework for data protection, in reality the protections offered by the IT Act and Rules were fraught with several limitations.

The first set of issues relate to the scope of Section 43A, which focused only on requirements of 'reasonable security practices' involving 'sensitive personal data' by 'body corporates'. The provision was, therefore, limiting in terms of the types of personal data covered, the exclusion of protections over and beyond data security and safety and the exclusion of government entities that did not fall within the provided definition of body corporates. The available information on cases under Section 43A points to the provision having been used mainly for claims on issues such as fraudulent transfer of funds from a person's bank account, unauthorised access to financial information, and information breaches related to falsely procured SIM cards.[35] Further, while the IT Rules adopted a broader view of data protection, as noted above, they did so by exceeding the ambit of the parent provision, that is, Section 43A of the IT Act that focused only on reasonable security safeguards.

It may appear that the early attention to reasonable security practices under Section 43A, which preceded the broader law on data protection, bears some resemblance to the Chinese approach where data security has been the first and foremost consideration. However, the driving force behind India's approach at that time was very different. The call for data security protections in the IT Act was prompted by the Indian IT services industry which found their outsourcing arrangements with foreign firms suffering due to the lack of data protection provisions in the domestic law. In the words of a government official, the aim was "*to bring in data privacy norms without increasing compliance costs for companies while allowing some leeway for contracts to address data security concerns*".[36]

Besides concerns of permissible scope, and a business-centric (rather than citizen-centric) intent the protections offered under the IT Act and Rules also suffered from problems of implementation, partly due to the limitations in the functioning of the adjudicatory mechanisms under the IT Act.[37] Taking account of all these factors, the Justice Srikrishna Committee acknowledged the insufficiency of the protections available under the IT Act and rules while recommending a new and comprehensive law on data protection.[38] Various other policy actors have echoed the need for an overarching data protection law, including through private member bills introduced in the Parliament and civil society led initiatives to propose the draft text of a privacy law.[39] These factors added to the momentum for the emergence of the new DPD Act, which once notified will replace Section 43A and the rules framed under it with a new framework for data protection.

---

[35] Divij Joshi, 'A Review of the Functioning of the Cyber Appellate Tribunal and Adjudicatory Officers under the IT Act' (Centre for Internet and Society, 6 June, 2014) <https://cis-india.org/internet-governance/blog/review-of-functioning-of-cyber-appellate-tribunal-and-adjudicatory-officers-under-it-act> accessed 19 April 2023.

[36] The Times of India, 'BPO will soon have some privacy' August 10 2004 <https://timesofindia.indiatimes.com/BPOs-will-soon-have-some-privacy/articleshow/806387.cms> accessed 1 April 2025.

[37] B.N. Srikrishna et al., A Free and Fair Digital Economy (n 8), 7

[38] Ibid.

[39] Amber Sinha, 'As India is Set to Implement its Data Protection Law. What to Make of It?' (Tech Policy Press, 28 March 2025) <https://www.techpolicy.press/as-india-is-set-to-implement-its-data-protection-law-what-to-make-of-it/> accessed 1 April 2025.

In addition, there are some sector specific norms that govern the confidentiality and protection of personal data in areas such as finance, telecommunications, and in the health sector.[40] These norms flow through a range of instruments that include legislations, rules, licence conditions and directives and are generally specific to particular types of data or use cases. To give a few examples, the Credit Information Companies (Regulation) Act, 2005 contains provisions for the accuracy, security, governing privacy principles and prevention of unauthorised access of credit information.[41] The Aadhaar digital identity project, described earlier, is now governed by the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, which lays down the requirements for the collection, use and sharing of personal data for its implementation.[42]

In the health space, statutory confidentiality protections are available for specific population groups under laws such as the Mental Healthcare Act, 2017 and the HIV and AIDS (Prevention and Control) Act, 2017.[43] Further, there are some non-statutory frameworks that apply to personal data protection in the digital health context. The Ayushman Bharat Digital Mission, a program for the digitization of health data in the country, has a Health Data Management Policy that sets out the standards of data protection to be followed by entities involved in the collection and sharing of health data.[44] In another example, during the Covid-19 pandemic the government launched a self-screening and contact tracing app called Aarogya Setu that involved the use of demographic data, patient health records, and location data for Covid management purposes. Responding to the public outcry over the lack of data privacy protections in this intervention, a committee set up by the government introduced a time-bound framework called the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020.[45] One of the main problems with such policies and protocols is the ease with which such protections can be withdrawn or altered. Their lack of statutory legitimacy also means a lack of effective enforcement structures to implement the protections.

1.4. Overview and analysis of the DPD Act, 2023

This section provides an overview of the DPD Act, drawing comparisons with the previous versions of the bills and highlighting some key issues. The DPD Act, 2023 contains 44 sections and is divided into 9 chapters. The broad scheme of the law is that it lays down the scope of the law, obligations of data fiduciaries, rights of data principals, and the framework for enforcement through the creation of DP Board. Unlike its predecessor bills from 2018 and 2019, the scope of the DPD Act is restricted to 'digital personal data' that is collected in a digital format or non-digital information that has subsequently been digitized.[46] This means that the law applies only to digitized data and excludes personal data that may be collected and stored using other means, such as in physical records. This is different from the practice followed in many other countries that apply more broadly to all types of processing of personal data,

---

[40] B.N. Srikrishna et al., 'White Paper of the Committee of Experts on Data Protection', <https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> accessed 19 April, 2023, 19-22.

[41] Credit Information Companies (Regulation) Act, 2005 <https://www.indiacode.nic.in/bitstream/123456789/2057/2/A200530.pdf> accessed 1 April 2025.

[42] Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 <https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_1307_2016.pdf> accessed 19 April 2023.

[43] Smriti Parsheera and B.N. Srikrishna, 'India's Legal Framework on Public Health and Privacy' in *Private and Controversial: When Privacy and Public Health Meet in India* (Smriti Parsheera, Harper Collins India Private Ltd, 2023).

[44] National Health Authority, 'National Digital Health Mission: Health Data Management Policy' (Ministry of Health and Family Welfare, April 2022) <https://abdm.gov.in/publications/policies_regulations/health_data_management_policy> accessed 19 April 2023.

[45] Empowered Group on Technology and Data Management, 'Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020' (Ministry of Electronics and Information Technology, 11 May 2020) <https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf> accessed 19 April 2023.

[46] DPD Act, s 3(a).

regardless of the means being used (for example, in Brazil).[47] Another way in which the Indian laws differs from other BRICS countries (and from its own precedent under Section 43A of the IT Act) is by avoiding any separate categorisation of sensitive personal data. The Act, however, follows the common practice of extending extraterritorial scope over the processing of digital data that takes place outside the country but relates to the offering goods or services to persons in India.[48]

As discussed in the introductory text, all versions of India's data protection bills have used the term "data fiduciary" to describe the entities that determine the purpose and means of processing of personal data and "data principal" to define the individual whose personal data is involved.[49] As explained by the Srikrishna Committee, this terminology is meant to clarify the role of the individual as the "focal actor in the digital economy" and to establish a duty of care and expectations of trust on the part of the entities processing the personal data.[50] While this approach stands apart from other BRICS counterparts that use terms like 'responsible party' (South Africa) and 'data controller' (Brazil) in their laws, the obligations being cast on Indian data fiduciaries and rights available to individuals are actually narrower in some respects. This will be illustrated in the discussions that follow.

Among its main obligations, the DPD Act contains requirements relating to notice to individuals about the collection and processing of data and obtaining their consent[51], to keep data accurate and complete[52], to implement appropriate technical and organisational measures to comply with the law.[53] The law also contains certain limitations on continuing retention of the data[54] and requires fiduciaries to maintain a mechanism for grievance redress.[55]

Further, the DPD requires data fiduciaries to undertake reasonable security safeguards to prevent the breach of personal data.[56] In an attempt to add some clarity to the meaning of 'reasonable security practices', the Draft Rules suggest that at a minimum such measures should include data security measures (use of encryption, obfuscation or masking techniques, etc), access controls and logs to monitor unauthorised access, and contractual arrangements with data processors to ensure security safeguards.[57] The exact design and scope of such practices is, however, left to be determined by the regulated entities with the DP Board having the power to impose a penalties for any observed failures in maintaining such safeguards.

In an improvement over the 2019 bill, the enacted law requires information about a breach to be conveyed to the DP Board as well as the affected data principals, in accordance with the rules to be made by the government.[58] In contrast, the previous draft suggested allowing the regulator to determine if and when individual breach notices should be given to the affected persons. The revised requirement of notice in all cases helps in granting individuals the agency to make their own decisions on how to deal with a breach situation in addition to any regulatory action. This may include personal risk mitigation strategies or the decision to discontinue transacting with a particular data fiduciary.

Like the versions before it, the DPD Act maintains a two-tier system of regulatory obligations, consisting of certain basic requirements for all covered actors and an enhanced set of obligations for significant data fiduciaries. The significance of such entities will be determined by the government based on factors like volume and sensitivity of data processed, risk of harm to individuals, sovereignty of the country,

---

[47] Article 3, General Law on the Protection of Personal Data (LGPD), 2018 <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> accessed 1 April 2025.
[48] DPD Act, s 3(b).
[49] DPD Act, 2023, ss 2(i) and 2(j).
[50] B.N. Srikrishna et al., A Free and Fair Digital Economy (n 8), 8.
[51] DPD Act, 2023, ss 5 and 6.
[52] DPD Act, 2023, s 8(3)(b).
[53] DPD Act, 2023, s 8(4).
[54] DPD Act, 2023, s 8(7).
[55] DPD Act, 2023, s 8(10).
[56] DPD Act, 2023, s 8(5).
[57] Draft Rules, rule 6.
[58] DPD Act, 2023, s 8(6).

electoral democracy, security of the state and public order.[59] This is in similar to China's practice of specifying additional principles to govern large Internet platform services and requirements of having data protection officers and independent oversight for entities that meet certain thresholds.[60]

Under the DPD Act, the additional requirements applicable to significant data fiduciaries include the conduct of data protection impact assessment, independent data audits and appointing a data protection officer.[61] As per the Draft Rules put out by the government, the DP Board would also need to be informed of any significant observations from the impact assessment or audit exercises. Further, the rules propose a new requirement of observance of due diligence by the significant data fiduciary while deploying of any algorithmic software for the processing of personal data, which might pose a risk to the rights of Data Principals.[62]

In addition to the consent of the user, the DPD Act recognises several other legitimate uses for data processing. The 2022 draft of the bill had introduced a new term called 'deemed consent' to capture all such situations, a list that seemed to consolidate the diffused list of exceptions under the previous versions of the draft law. The DPD Act does away with this specific term while retaining its concept. Its list of legitimate uses that can take place without consent begins with a 'reasonable expectation' clause to cover cases where an individual voluntarily furnishes their data to an entity and does not indicate the absence of consent for its processing.[63] The other grounds for legitimate processing include legally authorised state functions, grant of subsidies, benefits, certificates and licences, compliance with court orders, medical emergencies, public health and disasters, and purposes related to employment.[64]

Further, there are four specific rights made available to data principals – right to information about the processing of personal data, erasure and correction of information, access to grievance redress and right to appoint a nominee to take decisions in the event of death or incapacity of the individual.[65] Alongside these rights, the DPD Act introduces certain obligations for data principles. These obligations relate to compliance with applicable laws, not registering false or frivolous grievances, not furnishing any false particulars or suppressing material information and providing verifiably authentic information while seeing the correction or erasure of their data.[66] While it seems reasonable to expect that individuals should act in good faith while exercising their rights under the law, it is problematic to find that the law also allows for regulatory action to be taken against individuals for any violation of their duties.[67] This may result in a penalty of up to ten thousand rupees being imposed on the individual, which can be a deterrent in the exercise of their rights under the law.

Finally, the last few chapters of the law deal with the compliance and enforcement framework for data protection. The Act provides that compliance with the law will be administered by a new statutory board called the DP Board.[68] The main function of the DPB is to determine non-compliance with provisions of the law and impose penalties for any violation by data fiduciaries.[69] The bill lays down the procedure to be followed by the DP Board and lists the penalties that may be imposed for different types of violations. The highest penalty, which may extend up to two and a half billion rupees, has been indicated for a failure to take reasonable security safeguards to prevent a personal data breach.[70] An order made by

---

[59] DPD Act, 2023, s 10(1).
[60] Zhao Xinhua, Jerry Wang, Jane You and Dannie Sima, 'China Issues New Rules on Personal Information Compliance Audit' King and Wood Mallesons (20 February 2025) <https://www.kwm.com/cn/en/insights/latest-thinking/china-Issues-new-rules-on-personal-Information-compliance-audit.html> accessed 1 April 2025.
[61] DPD Act, 2023, s 10(2).
[62] Draft Rules, rule 12(3).
[63] DPD Act, 2023, s 7(a).
[64] DPD Act, 2023, s 7(b to i).
[65] DPD Act, 2023, ss 11 to 14.
[66] DPD Act, 2023, s 15.
[67] DPD Act, 2023, s 33(1) and the Schedule.
[68] DPD Act, 2023, s 18.
[69] DPD Act, 2023, s 27.
[70] DPD Act, 2023, schedule.

the DP Board may be challenged in appeal before an Appellate Tribunal. The DPD Act, 2023 designates the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) as the appropriate body for this purpose.[71] The TDSAT is an existing appellate authority with jurisdiction over matters relating to telecommunications, broadcasting, cyber appeals and airport tariffs.[72]

Having laid out the broad contours of the DPD Act, the next part of this section highlights some of the key issues with it. This discussion draws upon several concerns that the author has brought up (working alongside other collaborators) in response to various rounds of public consultation on the draft law.[73] The chapter focuses on a subset of these issues, which have been selected taking into account factors like the contested nature of those provisions (example — scope of government powers), the sweeping impact on human rights (example —broad exemptions for state agencies) and the importance for functioning and effectiveness of the proposed law (example —independence and accountability of the DP Board). However, this is by no means meant to serve as an exhaustive list of issues, many of which have been highlighted by other commentators.[74]

1.4.1. Diminished rights and protections

The DPD Act, which stands at 44 sections, is significantly shorter than the 98 sections that were seen in the 2019 version. While the number of sections does not in itself indicate robustness of a law, in the present case the shortened length does happen to be correlated with its reduced scope of protections.

First, the DPD Act, 2023 has done away with several of the rights and protections that were seen in PDP Bill, 2019 and were in line with internationally accepted norms of data protection. This includes the absence of provisions on collection limitation,[75] the right to portability of data[76] and the right to be forgotten[77], which are found in the laws of many other BRICS countries. It has also significantly diluted the standalone and explicit provision on purpose limitation seen in India's earlier bill.[78] Instead, the DPD Act, 2023 merges the purpose limitation requirement with the provision on consent.[79] The provision states that the consent given by the individual would be for the specified purpose and '*be limited to such personal data as is necessary for such specified purpose*'. This implies that the purpose limitation would apply only to those circumstances where it is necessary to obtain the individual's consent prior to processing their data. Similarly, the notice requirement under the law has also been diluted and intermeshed with the provision on consent. Section 5 of the DPD Act, 2023 provides that a data fiduciary has to give an

[71] DPD Act, 2023, ss 29 and 2(a).

[72] Telecom Disputes Settlement and Appellate Tribunal, Introduction about TDSAT < https://tdsat.gov.in/writereaddata/Delhi/docs/introduction.php?y=1> accessed 3 August 2023.

[73] Vrinda Bhandari et al., 'Response to the White Paper on a Data Protection Framework for India' (NIPFP, 2018) <https://macrofinance.nipfp.org.in/PDF/BKPRS2018WhitePaperResponse.pdf> accessed 19 April 2023; Rishab Bailey et al., 'Comments on the (Draft) Personal Data Protection Bill, 2018' (SSRN, 18 November 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269735>; Rishab Bailey et al., 'Comments on the (draft) Personal Data Protection Bill, 2019' (SSRN, 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051127> accessed 19 April 2023.

[74] 'Recommendations By SFLC.In On The Digital Personal Data Protection Bill 2022' (Software Freedom Law Center, India, 6 January 2023) <https://sflc.in/recommendations-sflcin-digital-personal-data-protection-bill-2022/> accessed 20 April 2023; Shailesh Gandhi, 'RTI Act Does Not Need Any Covert Amendment; it Needs Implementation' (News Click, 28 December 2022) <https://www.newsclick.in/RTI-act-need-covert-amendment-needs-implementation> accessed 20 April 2023; Akshit Chawla, 'Seven Issues With How The Data Protection Bill Safeguards Children's Data' (Medianama 17 December, 2022) <https://www.medianama.com/2022/12/223-seven-issues-data-protection-bill-childrens-data/> accessed 20 April 2023. 'GNI Comments to the Draft India Digital Personal Data Protection Bill, 2022' (Global Network Initiative, 4 February 2023) <https://globalnetworkinitiative.org/gni-comments-tothe-draft-india-digital-personal-data-protection-bill-2022/> accessed 20 April 2023.

[75] PDP Bill, 2019, s 6.

[76] PDP Bill, 2019, s 19.

[77] PDP Bill, 2019 Ibid.

[78] PDP Bill, 2019, s 4.

[79] DPD Act, 2023, s 6(1).

individual notice about the purpose of data collection and their legal rights while requesting for consent. This excludes the fairly large bucket of other 'legitimate uses'[80] that would be exempted from the purpose limitation and notice requirements under the DPD Act. It may be noted that the term 'legitimate uses' captures multiple use cases like data processing based on voluntary provision of data by an individual, processing for provision of subsidies, benefits and services by state agencies, and employment-related data processing. This is, however, different from the concept of 'legitimate interests' that appears as a standalone ground for data processing in the laws of some jurisdictions, such as Brazil.[81]

Second, the threshold of compliance being demanded from data fiduciaries has been diluted in many cases. For instance, the 2019 Bill required that the fiduciary 'shall take necessary steps' that the personal data being processed by it is accurate and complete.[82] The draft put out for consultation in 2022, however, diminished this to a requirement to make 'reasonable efforts' at ensuring accuracy.[83] This has been fixed by the DPD Act, 2023 to a requirement of ensuring completeness and accuracy but at the cost of limiting the protection to only two circumstances – where the processing is likely to make a decision that affects the individual or while disclosing data to another fiduciary.[84] Along the same vein, the requirement of 'necessary' security safeguards has been replaced with the standard of 'reasonable' safeguards.[85] The dilution in the expectations from data fiduciaries is accompanied by a new set of requirements on the duties expected to be followed by data principals, an interesting contrast given the goals of data protection.

The diluted scope of rights and protections is also accompanied by broad brush provisions that allow the government to exempt specified entities from the application of the DPD Act. Notably, Section 17(5) of the law enables the government to issue a notification within five years of its commencement to exempt 'such Data Fiduciary or classes of Data Fiduciaries' from any provision. The provision is silent on the grounds on which this provision may be triggered and open ended on the period for which such exemption can remain in effect. There is yet another provision that allows for a more limited exemption to be granted to notified entities, including startups, based on 'the volume and nature of personal data processed' by them.[86] The scope of this exemption extends to the requirements relating to notice, completeness, accuracy and retention of data, right to information access, and obligations for significant data fiduciaries.

1.4.2. Exemptions for state agencies

In addition to the exceptions mentioned above, which may apply to both public and private entities, there is another controversial provision that extends specifically to notified government agencies. It enables the government to declare that the provisions of the law will not apply to any 'instrumentality of the state' that may be identified by the government on certain grounds. These grounds are sovereignty and integrity of India, security of the State, friendly relations with foreign State, public order, or for preventing incitement to the commission of a serious offence relating to the above. A provision of this nature has existed in all the versions of India's data protection bills since 2019 and, for the reasons explained below, its problematic nature has only been enhanced by the text adopted in the 2023 Act.[87]

The existence of such a provision heightens the asymmetric relationship between the citizen and the State. Particularly so in light of the fact that law enforcement agencies in India already have very wide powers

---

[80] DPD Act, 2023, s 7.

[81] Bruno Ricardo Bioni, Mariana Rielli and Marina Kitayama, 'Legitimate interests under the Brazilian General Data Protection La: General framework and concrete examples' (Data Privacy Brazil Research, 2021) <https://fpf.org/wp-content/uploads/2021/07/LI-under-LGPD_Data-Privacy-Brasil-Research-Association-1.pdf> accessed 1 April 2025.

[82] PDP Bill, 2019, s 8(1).

[83] DPD Bill, 2022, s 9(2).

[84] DPD Act, 2023, s 8(3).

[85] PDP Bill, 2019, s 24(1) and DPD Act, 2023, s. 8(5).

[86] DPD Act, 2023, s 17(3).

[87] See PDP Bill, 2019, s 35, draft DPD Bill, 2022, s 18(2) and DPD Act, 2023, s 17(2)(a).

to access and intercept data without the protection of judicial oversight and other accountability and transparency measures.[88] The appropriate role of the data protection law should, therefore, have been to curb rather than strengthen these unchecked powers. While reviewing the 2019 Bill, several members of the JPC had also objected to the contents of this provision in their dissent notes on similar grounds.[89]

In our submissions on the 2019 version of the PDP Bill we recommended that if such a provision is to be retained in the draft it should be modified to specify the provisions of the data protection law that would continue to apply to exempted entities.[90] For instance, there seems to be little reason why requirements relating to clear and lawful purposes of processing, collection and retention limitations and data security safeguards should not be applicable to entities that are exempted for national security and public order related purposes. In addition, the exempted entity should be bound to put in place internal structures, such as the appointment of a retired judge as a judicial expert within the organisation, to approve any actions involving the processing of personal data by that agency.

Pending progress on the much-needed project of broader surveillance reforms in India, safeguards of the nature suggested above could have helped bring in some degree of checks on the personal data related actions of exempted government agencies. A similar proposal was put forward by the JPC member Manish Tewari in his dissent note. He proposed that any exemption under the provision should only be granted pursuant to a judicial approval from the appellate tribunal that was suggested under the 2019 version of the bill.[91] The DPD Bill, 2023 designates an existing body, the TDSAT, as the appellate tribunal for the purposes of the data protection law. While this body may not be the most suitable to consider data privacy related exemptions it would stilll be preferable to having the executive making these decisions without any independent oversight.

The DPD Act, however, does not incorporate any such safeguards. On the contrary, it fares worse than the previous versions on two main counts. First, it takes away some of the minimal safeguards that were suggested in the 2019 Bill, which had said that the government may specify certain procedures, safeguards and oversight mechanisms to be followed by the exempted agency. The JPC had suggested a further clarification that any procedure laid down by the government for the exempted agency should be a 'just, fair, reasonable and proportionate procedure'.[92] Second, the DPD Act, 2023 enables onward sharing of the personal data gathered by the exempted agency with the central government, with no limitation on the purposes for which it may be used by the government. It therefore expands the scope of the exemption much beyond the grounds stated earlier.

1.4.3. Impact on right to information

The DPD Act has diminished the scope of public transparency under the country's right to information law. The RTI Act is a transparency enhancing law that enables citizens to gain access to information that is under the control of public authorities. Public authorities are bound to respond to such information requests but this obligation is subject to certain exceptions, which includes respect for the privacy rights of the concerned individuals. As per this exception, public authorities would not be compelled to disclose any personal information that has no relationship to a public activity or interest or would cause unwarranted

---

[88] Software Freedom Law Center, India, 'India's Surveillance State: Communications Surveillance in India' (SFLCin and World Wide Web Foundation, 3 September 2014) <https://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf> accessed 20 April 2023; Rishab Bailey et. al., *Use of personal data by intelligence and law enforcement agencies*, (SSRN, 1 August 2018) <https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf> accessed 19 April 2023; Smriti Parsheera and Prateek Jha, 'Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?' (Carnegie India, 2020) <https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197> accessed 19 April 2023.

[89] Dissent notes by Manish Tewari, Gaurav Gogoi, Derek O'Brien and Mahua Moitra, RItesh Pandey, Jairam Ramesh, Vivek Tankha, and Amar Patnaik, in P.P. Chaudhary et al., 'Report of the Joint Committee' (n 30).

[90] Rishab Bailey et al., 'Comments on the (draft) Personal Data Protection Bill, 2019' (n 74).

[91] Dissent note by Manish Tewari, in P.P. Chaudhary et al., 'Report of the Joint Committee' (n 30), 216.

[92] P.P. Chaudhary et al., 'Report of the Joint Committee' (n 30), 120-121.

invasion of the privacy of the individual.[93] For instance, courts have observed that records pertaining to the performance of an employee/officer generally fall under the ambit of personal information and cannot be made available to members of the public as a matter of right.[94]

The aim of the exemption under the RTI Act was to maintain a balance between the right to public transparency and privacy of individuals. It did so by providing that the privacy exemption would not be absolute in nature and authorities under the RTI could require a disclosure of such information to be made if it served the larger public interest. The DPD Act has, however, done away with this balancing provision.[95] It amended the RTI Act to provide a blanket exception for any '*information which relates to personal information*'. The sweeping nature of this exemption will significantly diminish the scope of the right to information under the RTI Act as any information that relates to an identifiable person could be denied on the grounds of violating their privacy.

1.4.4. Concerns with the regulatory structure

The success of any data protection law depends, in large part, on effective implementation, which in turn depends on the functioning of the regulatory body created under it. In India's case this would include the balancing of the data protection body's independence from the government, which will comprise a large segment of the regulated entities, and its accountability to stakeholders, the government and the public. However, every successive draft of India's data protection bill has seen a weakening of the proposed regulatory framework and institutional mechanisms for data protection.

The 2019 bill proposed the creation of a new regulatory agency called the Data Protection Authority (DPA) that would consist of up to seven whole-time members. The powers of the DPA would have included making regulations to operationalise various aspects of the law and undertaking enforcement actions to ensure compliance with the statute and regulations. The selection of the DPA's members was to be done through a completely executive-led selection process (a committee of three senior officials from the government). Responding to the significant criticisms of this proposal, the JPC put forth a revised formulation including the following additional members – the Attorney General of India who is the country's senior most legal officer, an independent expert nominated by the government, and one director each from the Indian Institutes of Technology and Indian Institutes of Management.[96] This formulation, while marginally better, also did not go far enough in terms of ensuring the independence of the selection process from government control.

DPD Act, 2023, however, does away with the earlier formulations while opting for a weakened regulatory structure. First, it replaces the concept of the DPA with a DP Board where the number of members on the board, their process of selection, process of functioning will all be prescribed later by the government.[97] The Draft Rules put out in January 2025 have introduced the proposed provisions in this regard. By refusing to address these provisions in the primary law (as opposed to the rules) the statute errs in achieving the independence of this body from the government. This is because unlike the statue, which can be amended only through a legislative process, the rules can be modified more easily by the executive at any point of time. The 2023 Act, however, did make an improvements over its 2022 draft which suggested that even things like the qualifications of board members would be left to be determined by the government.[98]

Second, the role of the DP Board has also been curtailed, mainly to deal with data breaches and determining non-compliance with provisions of the law.[99] Unlike the previously imagined DPA, the DP

[93] RTI Act, 1995, s 8(1)(j).
[94] *Girish Ramchandra Deshpande* v. *Central Information Commissioner*, (2013) 1 SCC 212.
[95] DPD Act, 2023, s 44(3)
[96] P.P. Chaudhary et al., 'Report of the Joint Committee' (n 30), 128-129.
[97] DPD Act, 2023, s 19 (1) and (2) and s 23(1).
[98] DPD Bill, 2022, s 19(2).
[99] DPD Act, 2023, s 27.

Board will not have any regulation-making powers. This distinguishes the Indian DP Board from the authorities created under the data protection laws of other BRICS countries that have the power to frame regulations on different aspects of the law. The DPD Act's institutional design effectively enhances the powers that will be available in the hands of the government, allowing it to issue clarifications, restrictions, and rules on the interpretation and scope of the data protection law. For instance, the law states that the government will make rules on issues as varied as deciding upon the suitable time period for data retention,[100] designation of significant data fiduciaries,[101] and notification of restricted countries for cross border data flows.[102] Each of these constitutes a significant power that can substantially reshape the obligations of regulated entities and the scope of individual rights. But the DPD Act does not cast any obligations of public consultation, cost-benefit analysis, or other forms of due process in the actions of the government while making such decisions.

1.4.5. Cross border data flows

The topic of cross border data flows has been one of the most contested aspects of the Indian data protection debate. The initial drafts of the bill began with the suggestion of imposing fairly strict localization requirements for certain types of data, which would have to be compulsorily stored on local Indian servers, and conditional data transfer models for the rest. However, these proposals were eventually relaxed in favour of the current position under Section 16 of the DPD Act. The provision allows personal data to be freely transferred, except to any restricted countries that may be notified by the government. Popularly referred to as the 'blacklisting' approach, India's final approach is more liberal compared to that of any of the other BRICS countries that contain provisions on prior consent, adequacy of the other country's laws, standard contractual clauses, and certification as available mechanisms for the transfer personal data outside the country.

The DPD Act's seemingly liberal position, however, comes with an important caveat. The law clarifies that its open position on cross border flows will not restrict the operation of any other laws that may contain '*a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof*'.[103] This clarification is important for two reasons. First, the provision preserves the space for sector-specific localization provisions, a fairly large number of which are already in place in India in sectors like payments, telecommunications, cloud storage of government data, and books of accounts of companies.[104] Second, the Draft Rules interpret this provision, and the DPD Act more generally, to mean that government can also introduce additional restrictions on data flows through new rules.

Notably, the Draft Rules provide that any transfer of data to '*any foreign State, or to any person or entity under the control of or any agency of such a State*' will be subject to the restrictions specified in any order issued by the government.[105] The rules also prescribe a separate requirement that significant data fiduciaries will be bound by any restrictions on the flow of '*personal data and the traffic data pertaining to its flow*' that may be imposed by the government on the recommendations of a committee constituted by it.[106] In both these cases the Draft Rules defer the specifics of the nature of the restriction that would be applicable hence creating ambiguity around the practical implications of the liberal provision on cross border flows adopted by the DPD Act.

---

[100] DPD Act, 2023 s 8(8).
[101] DPD Act, 2023, s 10.
[102] DPD Act, 2023, s 16.
[103] DPD Act, 2023, s 16(2).
[104] Smriti Parsheera, 'Country Deep Dive: India' in Global Governance of Cross-Border Data Flows: Operationalising Practical Solutions: A Compendium of Research Papers (Centre on Regulation in Europe, 2024) <https://cerre.eu/wp-content/uploads/2024/09/240905_CBDT_FullBook_FINAL.pdf> accessed 1 April 2025.
[105] Draft Rules, rule 14.
[106] Draft Rules, rule 12(4).

1.5. Other developments: Architectures and proposals on data governance

As the legislative proposal on personal data protection remained in a state of flux, there were at least two other relevant developments that intersected with the discussions on data protections. The first development related to the initiation of policy discussions around the regulation of 'non-personal data' in India. Non-personal data in this context refers either to personally identifiable data that has been anonymized or data which by its nature was never personal in nature. Examples include anonymised health data of patients, land records, vehicle registration details, etc. In the 2019 version of the bill the government introduced a provision, Section 91, that would allow them to direct any data fiduciary to furnish any anonymised personal data or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies.[107]

This change was introduced even though the government had already constituted a separate expert committee headed by Kris Gopalakrishnan to make recommendations on the governance of non-personal data.[108] As per the recommendations of this committee, government and private organisations that collect and manage data should be bound by certain requirements like sharing details of the meta data collected by them and making data sets that are designated as high-value datasets available to requesting entities. The Gopalkrishnan committee recommended the creation of a separate legal framework and statutory authority to oversee the governance of non-personal data.

The JPC, however, was of the opinion that not only should Section 91 of the PDP Bill, 2019 remain, there should be an overall expansion in the scope of the law so as to cover both personal and non-personal data. To support this idea the JPC pointed to the impossibility of making clear demarcations between personal and non-personal data, which would lead to regulatory uncertainty and complications. Several members of the JPC, however, opposed this idea in their dissent notes.[109] In alignment with these dissenting voices, the DPD Act limits its scope to digital personal data keeping any references to non-personal data out of its scope. With this, the intermingling of the policy conversations on personal and non-personal data can be said to have been settled for now although we still do not have clarity about how India will finally choose to regulate non-personal data.

The second important development relates to India's adoption of a technical architecture on consent management called the Data Empowerment and Protection Architecture (DEPA), which represents the consent layer of India Stack.[110] This refers to a model of electronic consent management and sharing of data based on the consent of the individual. The electronic consent under DEPA is to be collected, stored and managed by intermediaries called consent managers who are proposed to be regulated under the data protection bill. The DPD Act defines consent managers as a person that enables an individual to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform.[111] Such consent managers will have to be registered with the DP Board and be bound by the technical, operational, and financial conditions to be notified by the government.[112] The Draft Rules accordingly lay down the conditions of registration for consent managers.[113]

While the DPD Act now gives legal sanctity to the institution of consent managers and the rules governing them are in the process of being framed, the adoption of the DEPA framework is already underway in many sectors. This is notably the case in the financial sector, under the account aggregators regulations,

---

[107] PDP Bill, 2019, s 91.

[108] Kris Gopalakrishnan et. al., 'Report by the Committee of Experts on Non-Personal Data Governance Framework' (Ministry of Electronics and Information Technology, December 2020) 20 <https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf> accessed 19 April 2023.

[109] Dissent notes by Gaurav Gogoi, Derek O'Brien and Mahua Moitra, in P.P. Chaudhary et al., 'Report of the Joint Committee' (n 30), 223-228, 219-220.

[110] NITI Aayog, 'Data Empowerment and Protection Architecture: Draft for Discussion' (2020) <https://www.niti.gov.in/sites/default/ files/2020-09/DEPA-Book.pdf> accessed 20 April 2023.

[111] DPD Act, 2023, s 2(g).

[112] DPD Act, 2023, s 6(9).

[113] Draft Rules, rule 4 and First Schedule.

and under the Ayushman Bharat Digital Health Mission for the sharing of digital health records.[114] The advantages of such a framework include the generation of verifiable consent logs that can bring in better accountability in the present system of consent. It can also bring in more efficiency and transparency in the sharing of data through the use of application programming interfaces (APIs).[115] At the same time the increasing footprint of this architecture also raises questions about its role in incentivizing more and more collection and sharing of data without being able to address many of the structural problems with the over-reliance on consent as the basis of data processing.[116] Further, the roll out of DEPA, which began before a data protection law was in place, illustrated the expedited policy track for the implementation of technical architectures in India while necessary legal structures continue to take a back seat.

1.6. Automated Personal Data Processing

The scope of the Indian data protection law covers automated processing, which implies that all of the provisions of the law extend to automated processing. To elaborate, the term 'data' is defined as any 'representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means'.[117] Further, the term 'automated' has also been defined in the law. It refers to a 'digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data'.[118] Both wholly and partly automated operations involving personal data qualify as 'processing' under the DPD Act.[119] The law, however, does not contain any enhanced rights in the context of automated processing such as the right not to be subject to a decision based solely on automated processing, which is found in the data protection laws of countries like Brazil and South Africa and in the European GDPR.

However, as per official accounts, some elements of the intersection between AI and data protection will be covered by a proposed new law on digital governance, which is being referred to as the proposed Digital India Act. As per a presentation put out by the government in February, 2023, the scope of the Digital India Act would include the definition and regulation of high risk AI systems, AI based ad targeting and content moderation, and protections against automated decision making.[120] But this proposal has not seen much policy movement since then and its future remains uncertain.

Further, India has not yet adopted any specialised legal framework on the regulation of artificial intelligence (AI) although the government has issued some advisories on the subject.[121] Some of these advisories have been controversial on account of their intrusive and sweeping directions and lack of legislative backing. For instance, one such advisory, which was subsequently withdrawn in light of significant pushback from the industry and civil society, called for prior government approval for the deployment of any untested or unreliable AI models.[122]

---

[114] Reserve Bank of India, 'Reserve Bank of India, Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions' (2016) <https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598> accessed 20 April 2023; National Health Authority, 'National Digital Health Mission: Health Data Management Policy' (n 44).

[115] Tripti Jain, 'Tech Tools to Facilitate and Manage Consent: Panacea or Predicament? A Feminist Perspective' (Data Governance Network, December 2021) <https://internetdemocracy.in/reports/tech-tools-to-facilitate-and-manage-consent> accessed 20 April 2022; Smriti Parsheera, 'An Analysis of India's New Data Empowerment Architecture' in *Emerging Trends in Data Governance* (Centre for Communication Governance, January 2023) 7-24 <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-edited-volume-emerging-trends-in-data-governance-343.pdf> accessed 19 April 2023.

[116] Ibid.

[117] DPD Act, 2023, s 2(h).

[118] DPD Act, 2023, s 2(h).

[119] DPD Act, 2023, s 2(x).

[120] Ministry of Electronics and Information Technology, Government of India, 'Proposed Digital India Act, 2023' <https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf> accessed 1 November 2024.

[121] Arjun Adrian D'Souza, 'India's foray into regulating AI', IAPP (24 April 2024) <https://iapp.org/news/a/indias-foray-into-regulating-ai> accessed 1 November 2024.

[122] Ibid.

The country has also seen a series of policy conversations on the development and deployment of responsible AI systems. These initiatives have been led by the government think tank, NITI Aayog. The list of policy documents includes a National Strategy for Artificial Intelligence released in June 2018, the Principles for Responsible AI issued in February 2021 and a document on Operationalizing the Principles for Responsible AI that followed in August that year.[123] These developments, however, maintain the status of non-binding guidelines on AI and do not point to any movement toward the adoption of a regulatory framework on the subject. In summary, the future of India's legal framework on AI remains unclear at this point. Yet, we continue to see extensive deployment of automated technologies in the private sector and surrounding the use of computer systems to support government administration.[124]

1.7. Conclusion

A modern and comprehensive data protection law has been a long pending necessity for India. It is necessary for protecting the fundamental rights of citizens, checking the data excesses committed by state agencies and private actors and ensuring global competitiveness. The task of translating this well-recognized need into a legislative reality has, however, taken much longer than it ought to have. This chapter offered a brief history of India's attempts at formulating a law on data protection, a trajectory that was marred by a series of uncertainties and delays until the eventual adoption of the DPD Act in August, 2023.

The manner in which a new bill was hurriedly rushed through Parliament without effective Parliamentary deliberations or public consultation on new ideas saw the undoing of a half-decade long consultation process. As discussed in the chapter, the law, as enacted, contains several limitations in the scope of rights and protections being offered and provisions for government exemptions. But, despite these limitations, the DPD Act signals a new dawn for data protection in India.

The Indian DPD Act reflects some parallels with the laws of other BRICS countries that have been studied in this collection of essays. For instance, through its differential treatment of data fiduciaries based on their size and relevance -- additional requirements for significant data fiduciaries and possible exemptions for startups and small businesses. This is similar to China's differential treatment of large Internet platform services and the direction under the Brazilian law to facilitate compliance with the data protection law by small businesses and micro-enterprises. Similarly, the focus on data localization in the Indian policy discourse is similar to the attention received by this subject in countries like China and Russia although India's final approach on cross-border flows has turned out to be different from all the other BRICS countries.

There are several other reasons that make the Indian approach stand out from the other BRICS countries. First, as discussed in the chapter, the country is trailing behind in terms of the pace of adoption of its data protection law, which is still a work in progress while all the other jurisdictions already have a functional data protection framework in place. The institutional design of the Indian law also differs given its choice of creating a Data Protection Board with a limited set of functions, instead of a full fledged regulatory authority as is seen in most other jurisdictions. Additionally, unlike most other data protection laws that cover all types of personal data, the scope of the DPD Act is limited only to digital data. There are also other differences in the terminology adopted by the law (using terms like data fiduciaries and principals) and the scope of rights and protections (no right to be forgotten, right to data portability, or restrictions on decisions based solely on automated processing).

Crucially, the Indian experience also stands out in terms of its 'tech-first approach' to digital governance. Over the last decade and a half the country has seen a move towards greater reliance on state-endorsed technology solutions to achieve societal objectives in areas like digital identity, digital payments and most

[123] White & Case, AI Watch: Global regulatory tracker - India (13 May 2024) <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-india> accessed 1 November 2024.
[124] Divij Joshi, AI Observatory, 'The Legal, Institutional, & Technical Architecture of ADMS in India' <https://ai-observatory.in/> accessed 1 November 2024.

recently consent management. The creation of the institution of consent managers under the DPD Act is also a part of this trend. While a technical architecture that is designed to bring greater accountability in consent collection and data sharing is a valuable tool, it is not sufficient to meet the overall goals of a holistic data protection framework.

The enactment of the DPD Act and its adoption of the consent management framework are, therefore ,only the first steps towards the dawn of meaningful data protection in the country. This will have to be followed by the arduous process of creating the new statutory board, framing sound rules to give effect to several important aspects of the law, and building compliance capacity among stakeholders. The DPD Act makes an important start in this direction, albeit with an incomplete set of protections that will have to be refined and improved with time. It is possible that this law will be challenged, revisited and refined in the coming years through legislative or judicial interventions. In parallel, there is much to be done in terms of institution building and rule-making to give life to the new law.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

2. APPENDIX A – THE DIGITAL PERSONAL DATA PROTECTION ACT

(No. 22 of 2023)
[August 11th, 2023]

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

Chapter I
Preliminary

1. (1) This Act may be called the Digital Personal Data Protection Act, 2023.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

2. In this Act, unless the context otherwise requires,—

(a) "Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997;

(b) "automated" means any digital process capable of operating automaticallyin response to instructions given or otherwise for the purpose of processing data;

(c) "Board" means the Data Protection Board of India established by the CentralGovernment under section 18;

(d) "certain legitimate uses" means the uses referred to in section 7;

(e) "Chairperson" means the Chairperson of the Board;

(f) "child" means an individual who has not completed the age of eighteenyears;

(g) "Consent Manager" means a person registered with the Board, who acts asa single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform;

(h) "data" means a representation of information, facts, concepts, opinions orinstructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;

(i) "Data Fiduciary" means any person who alone or in conjunction with otherpersons determines the purpose and means of processing of personal data;

(j) "Data Principal" means the individual to whom the personal data relates andwhere such individual is—

(i) a child, includes the parents or lawful guardian of such a child;

(ii) a person with disability, includes her lawful guardian, acting on herbehalf;

(k) "Data Processor" means any person who processes personal data on behalfof a Data Fiduciary;

(l) "Data Protection Officer" means an individual appointed by the SignificantData Fiduciary under clause (*a*) of sub-section (*2*) of section 10;

(m) "digital office" means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;

(n) "digital personal data" means personal data in digital form;(*o*) "gain" means—

(i) a gain in property or supply of services, whether temporary orpermanent; or

(ii) an opportunity to earn remuneration or greater remuneration or togain a financial advantage otherwise than by way of legitimate remuneration;

(*p*) "loss" means—

(i) a loss in property or interruption in supply of services, whethertemporary or permanent; or

(ii) a loss of opportunity to earn remuneration or greater remuneration orto gain a financial advantage otherwise than by way of legitimate remuneration; (*q*) "Member" means a Member of the Board and includes the Chairperson;

(*r*) "notification" means a notification published in the Official Gazette and the expressions "notify" and "notified" shall be construed accordingly; (*s*) "person" includes—

(i) an individual;

(ii) a Hindu undivided family;

(iii) a company;

(iv) a firm;

(v) an association of persons or a body of individuals, whetherincorporated or not;

(vi) the State; and

(vii) every artificial juristic person, not falling within any of the precedingsub-clauses;

(t) "personal data" means any data about an individual who is identifiable by orin relation to such data;

(u) "personal data breach" means any unauthorised processing of personaldata or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;

(v) "prescribed" means prescribed by rules made under this Act;

(w) "proceeding" means any action taken by the Board under the provisions ofthis Act;

(x) "processing" in relation to personal data, means a wholly or partly automatedoperation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

(y) "she" in relation to an individual includes the reference to such individualirrespective of gender;

(z) "Significant Data Fiduciary" means any Data Fiduciary or class of DataFiduciaries as may be notified by the Central Government under section 10;

(*za*) "specified purpose" means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder; and

(*zb*) "State" means the State as defined under article 12 of the Constitution.

3. Subject to the provisions of this Act, it shall—
(*a*) apply to the processing of digital personal data within the territory of India where the personal data is collected—

(i) in digital form; or

(ii) in non-digital form and digitised subsequently;

(b) also apply to processing of digital personal data outside the territory ofIndia, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;

(c) not apply to—

(i) personal data processed by an individual for any personal or domesticpurpose; and

(ii) personal data that is made or caused to be made publicly available by—

(A) the Data Principal to whom such personal data relates; or

(B) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Illustration.

X, an individual, while blogging her views, has publicly made available her personal data on social media. In such case, the provisions of this Act shall not apply.

CHAPTER II
OBLIGATIONS OF DATA FIDUCIARY

4. (*1*) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—

(*a*) for which the Data Principal has given her consent; or (*b*) for certain legitimate uses.

(*2*) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.

5. (*1*) Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her,—

(i) the personal data and the purpose for which the same is proposed to be processed;

(ii) the manner in which she may exercise her rights under sub-section (*4*) of section 6 and section 13; and

(iii) the manner in which the Data Principal may make a complaint to the Board,

in such manner and as may be prescribed.

Illustration.

X, an individual, opens a bank account using the mobile app or website of Y, a bank. To complete the Know-Your-Customer requirements under law for opening of bank account, X opts for processing of her personal data by Y in a live, video-based customer identification process. Y shall accompany or precede the request for the personal data with notice to X, describing the personal data and the purpose of its processing.

(*2*) Where a Data Principal has given her consent for the processing of her personal data before the date of commencement of this Act,—

(*a*) the Data Fiduciary shall, as soon as it is reasonably practicable, give to the Data Principal a notice informing her,—

(i) the personal data and the purpose for which the same has been processed;

(ii) the manner in which she may exercise her rights under sub-section (*4*) of section 6 and section 13; and

(iii) the manner in which the Data Principal may make a complaint to the Board,

in such manner and as may be prescribed.

(*b*) the Data Fiduciary may continue to process the personal data until and unless the Data Principal withdraws her consent.

Illustration.

X, an individual, gave her consent to the processing of her personal data for an online shopping app or website operated by Y, an e-commerce service provider, before the commencement of this Act. Upon commencement of the Act, Y shall, as soon as practicable, give through email, in-app notification or other effective method information to X, describing the personal data and the purpose of its processing.

(*3*) The Data Fiduciary shall give the Data Principal the option to access the contents of the notice referred to in sub-sections (*1*) and (*2*) in English or any language specified in the Eighth Schedule to the Constitution.

6. (*1*) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

Illustration.

X, an individual, downloads Y, a telemedicine app. Y requests the consent of X for (*i*) the processing of her personal data for making available telemedicine services, and (*ii*) accessing her mobile phone contact list, and X signifies her consent to both. Since phone contact list is not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services.

(2) Any part of consent referred in sub-section (*1*) which constitutes an infringement of the provisions of this Act or the rules made thereunder or any other law for the time being in force shall be invalid to the extent of such infringement.

Illustration.

X, an individual, buys an insurance policy using the mobile app or website of Y, an insurer. She gives to Y her consent for (*i*) the processing of her personal data by Y for the purpose of issuing the policy, and (*ii*) waiving her

right to file a complaint to the Data Protection Board of India. Part (*ii*) of the consent**,** relating to waiver of her right to file a complaint, shall be invalid.

(3) Every request for consent under the provisions of this Act or the rules madethereunder shall be presented to the Data Principal in a clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act.

(4) Where consent given by the Data Principal is the basis of processing of personaldata, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.

(5) The consequences of the withdrawal referred to in sub-section (*4*) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

Illustration.

X, an individual, is the user of an online shopping app or website operated by Y, an e-commerce service provider. X consents to the processing of her personal data by Y for the purpose of fulfilling her supply order and places an order for supply of a good while making payment for the same. If X withdraws her consent, Y may stop enabling X to use the app or website for placing orders, but may not stop the processing for supply of the goods already ordered and paid for by X.

(6) If a Data Principal withdraws her consent to the processing of personal data undersub-section (*5*), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such processing without her consent is required or authorised under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India.

Illustration.

X, a telecom service provider, enters into a contract with Y, a Data Processor, for emailing telephone bills to the customers of X. Z, a customer of X, who had earlier given her consent to X for the processing of her personal data for emailing of bills, downloads the mobile app of X and opts to receive bills only on the app. X shall itself cease, and shall cause Y to cease, the processing of the personal data of Z for emailing bills.

(7) The Data Principal may give, manage, review or withdraw her consent to the DataFiduciary through a Consent Manager.

(8) The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed.

(9) Every Consent Manager shall be registered with the Board in such manner andsubject to such technical, operational, financial and other conditions as may be prescribed.

(10) Where a consent given by the Data Principal is the basis of processing ofpersonal data and a question arises in this regard in a proceeding, the Data Fiduciary shall be obliged to prove that a notice was given by her to the Data Principal and consent was given by such Data Principal to the Data Fiduciary in accordance with the provisions of this Act and the rules made thereunder.

7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:—

(*a*) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data.

Illustrations.

(I) X, an individual, makes a purchase at Y, a pharmacy. She voluntarily provides Y herpersonal data and requests Y to acknowledge receipt of the payment made for the purchase by sending a message to her mobile phone. Y may process the personal data of X for the purpose of sending the receipt.

(II) X, an individual, electronically messages Y, a real estate broker, requesting Y tohelp identify a suitable rented accommodation for her and shares her personal data for this purpose. Y may process her personal data to identify and intimate to her the details of accommodation available on rent. Subsequently, X informs Y that X no longer needs help from Y. Y shall cease to process the personal data of X;

(*b*) for the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where–
–

(i)she has previously consented to the processing of her personal databy the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or

(ii) such personal data is available in digital form in, or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government, subject to standards followed for processing being in accordance with the policy issued by the Central Government or any law for the time being in force for governance of personal data.

Illustration.

X. a pregnant woman, enrols herself on an app or website to avail of government's maternity benefits programme, while consenting to provide her personal data for the purpose of availing of such benefits. Government may process the personal data of X processing to determine her eligibility to receive any other prescribed benefit from the government;

(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;

(d) for fulfilling any obligation under any law for the time being in force in Indiaon any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

(e) for compliance with any judgment or decree or order issued under any lawfor the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

(f) for responding to a medical emergency involving a threat to the life orimmediate threat to the health of the Data Principal or any other individual;

(g) for taking measures to provide medical treatment or health services to anyindividual during an epidemic, outbreak of disease, or any other threat to public health;

(h) for taking measures to ensure safety of, or provide assistance or services to**,** any individual during any disaster, or any breakdown of public order.

Explanation.—For the purposes of this clause, the expression "disaster" shall have the same meaning as assigned to it in clause (*d*) of section 2 of the Disaster 53 of 2005. Management Act, 2005; or

(i) for the purposes of employment or those related to safeguarding the employerfrom loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

8. (*1*) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor.

(2) A Data Fiduciary may engage, appoint, use or otherwise involve a Data Processorto process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract.

(3) Where personal data processed by a Data Fiduciary is likely to be—

(b) used to make a decision that affects the Data Principal; or

(c) disclosed to another Data Fiduciary,the Data Fiduciary processing such personal data shall ensure its completeness, accuracy and consistency.

(4) A Data Fiduciary shall implement appropriate technical and organisational measuresto ensure effective observance of the provisions of this Act and the rules made thereunder.

(5) A Data Fiduciary shall protect personal data in its possession or under its control,including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

(6) In the event of a personal data breach, the Data Fiduciary shall give the Board andeach affected Data Principal, intimation of such breach in such form and manner as may be prescribed.

(7) A Data Fiduciary shall, unless retention is necessary for compliance with any lawfor the time being in force,—

(d) erase personal data, upon the Data Principal withdrawing her consent or as

soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and

(e) cause its Data Processor to erase any personal data that was made availableby the Data Fiduciary for processing to such Data Processor.

Illustrations.

(I) X, an individual, registers herself on an online marketplace operated by Y, ane-commerce service provider. X gives her consent to Y for the processing of her personal data for selling her used car. The online marketplace helps conclude the sale. Y shall no longer retain her personal data.

(II) X, an individual, decides to close her savings account with Y, a bank. Y is requiredby law applicable to banks to maintain the record of the identity of its clients for a period of ten years beyond closing of accounts. Since retention is necessary for compliance with law, Y shall retain X's personal data for the said period.

(8) The purpose referred to in clause (*a*) of sub-section (*7*) shall be deemed to no longer be served, if the Data Principal does not—

(f)approach the Data Fiduciary for the performance of the specified purpose; and

(g) exercise any of her rights in relation to such processing, for such time period as may be prescribed, and different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes.

(9) A Data Fiduciary shall publish, in such manner as may be prescribed, the businesscontact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions, if any, raised by the Data Principal about the processing of her personal data.

(10) A Data Fiduciary shall establish an effective mechanism to redress the grievancesof Data Principals.

(11) For the purposes of this section, it is hereby clarified that a Data Principal shall beconsidered as not having approached the Data Fiduciary for the performance of the specified purpose, in any period during which she has not initiated contact with the Data Fiduciary for such performance, in person or by way of communication in electronic or physical form.

9. (*1*) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed. *Explanation.*—For the purpose of this sub-section, the expression "consent of the parent" includes the consent of lawful guardian, wherever applicable.

(2) A Data Fiduciary shall not undertake such processing of personal data that islikely to cause any detrimental effect on the well-being of a child.

(3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of childrenor targeted advertising directed at children.

(4) The provisions of sub-sections (*1*) and (*3*) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.

(5) The Central Government may, if satisfied that a Data Fiduciary has ensured that itsprocessing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (*1*) and (*3*) in respect of processing by that Data Fiduciary as the notification may specify.

10. (*1*) The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including—

(a) the volume and sensitivity of personal data processed;

(b) risk to the rights of Data Principal;

(c) potential impact on the sovereignty and integrity of India;

(d) risk to electoral democracy;

(e) security of the State; and(*f*) public order.

(*2*) The Significant Data Fiduciary shall—

(a) appoint a Data Protection Officer who shall—

(i) represent the Significant Data Fiduciary under the provisions of thisAct;

(ii) be based in India;

(iii) be an individual responsible to the Board of Directors or similargoverning body of the Significant Data Fiduciary; and

(iv) be the point of contact for the grievance redressal mechanism underthe provisions of this Act;

(b) appoint an independent data auditor to carry out data audit, who shallevaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act; and

(c) undertake the following other measures, namely:—

(i) periodic Data Protection Impact Assessment, which shall be a processcomprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals, and such other matters regarding such process as may be prescribed;

(ii) periodic audit; and

(iii) such other measures, consistent with the provisions of this Act, asmay be prescribed.

CHAPTER III
RIGHTS AND DUTIES OF DATA PRINCIPAL

11. (*1*) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (*a*) of section 7 (hereinafter referred to as the said Data Fiduciary), for processing of personal data, upon making to it a request in such manner as may be prescribed, —

(a) a summary of personal data which is being processed by such Data Fiduciaryand the processing activities undertaken by that Data Fiduciary with respect to such personal data;

(b) the identities of all other Data Fiduciaries and Data Processors with whomthe personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

(c) any other information related to the personal data of such Data Principal andits processing, as may be prescribed.

(*2*) Nothing contained in clause (*b*) or clause (*c*) of sub-section (*1*) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorised by law to obtain such personal data, where such sharing is pursuant to a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

(*3*) For the purposes of this section, the expression "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act or the rules made thereunder due to unsoundness of mind or infirmity of body.

12. (*1*) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (*a*) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(2) A Data Fiduciary shall, upon receiving a request for correction, completion orupdating from a Data Principal,—

(a) correct the inaccurate or misleading personal data;

(b) complete the incomplete personal data; and(*c*) update the personal data.

(3) A Data Principal shall make a request in such manner as may be prescribed to theData Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

13. (*1*) A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of her rights under the provisions of this Act and the rules made thereunder.

(2) The Data Fiduciary or Consent Manager shall respond to any grievances referredto in sub-section (*1*) within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries.

(3) The Data Principal shall exhaust the opportunity of redressing her grievanceunder this section before approaching the Board.

14. (*1*) A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act and the rules made thereunder.

15. A Data Principal shall perform the following duties, namely:—

(a) comply with the provisions of all applicable laws for the time being in forcewhile exercising rights under the provisions of this Act;

(b) to ensure not to impersonate another person while providing her personaldata for a specified purpose;

(c) to ensure not to suppress any material information while providing herpersonal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;

(d) to ensure not to register a false or frivolous grievance or complaint with aData Fiduciary or the Board; and

(e) to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure under the provisions of this Act or the rules made thereunder.

CHAPTER IV
SPECIAL PROVISIONS

16. (*1*) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

(*2*) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of

protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

17. (*1*) The provisions of Chapter II, except sub-sections (*1*) and (*5*) of section 8, and those of Chapter III and section 16 shall not apply where—

(a) the processing of personal data is necessary for enforcing any legal right orclaim;

(b) the processing of personal data by any court or tribunal or any other bodyin India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function;

(c) personal data is processed in the interest of prevention, detection,investigation or prosecution of any offence or contravention of any law for the time being in force in India;

(d) personal data of Data Principals not within the territory of India is processedpursuant to any contract entered into with any person outside the territory of India by any person based in India;

(e) the processing is necessary for a scheme of compromise or arrangement ormerger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force; and

(f) the processing is for the purpose of ascertaining the financial informationand assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force.

Explanation.—For the purposes of this clause, the expressions "default" and "financial institution" shall have the meanings respectively assigned to them in sub-sections (*12*) and (*14*) of section 3 of the Insolvency and Bankruptcy Code, 2016. *Illustration.*

X, an individual, takes a loan from Y, a bank. X defaults in paying her monthly loan repayment instalment on the date on which it falls due. Y may process the personal data of X for ascertaining her financial information and assets and liabilities.

(2) The provisions of this Act shall not apply in respect of the processing of personaldata—

(*a*) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and (*b*) 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 and such processing is carried on in accordance with such standards as may be prescribed.

(3) The Central Government may, having regard to the volume and nature of personaldata processed, notify certain Data Fiduciaries or class of Data Fiduciaries, including startups, as Data Fiduciaries to whom the provisions of section 5, sub-sections (*3*) and (*7*) of section 8 and sections 10 and 11 shall not apply.

Explanation.—For the purposes of this sub-section, the term "startup" means a private limited company or a partnership firm or a limited liability partnership incorporated in India, which is eligible to be and is recognised as such in accordance with the criteria and process notified by the department to which matters relating to startups are allocated in the Central Government.

(4) In respect of processing by the State or any instrumentality of the State, the provisions of sub-section (*7*) of section 8 and sub-section (*3*) of section 12 and, where such processing is for a purpose that does not include making of a decision that affects the Data Principal, sub-section (*2*) of section 12 shall not apply.

(5) The Central Government may, before expiry of five years from the date ofcommencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CHAPTER V
DATA PROTECTION BOARD OF INDIA

18. (*1*) With effect from such date as the Central Government may, by notification, appoint, there shall be established, for the purposes of this Act, a Board to be called the Data Protection Board of India.

(2) The Board shall be a body corporate by the name aforesaid, having perpetualsuccession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

(3) The headquarters of the Board shall be at such place as the Central Governmentmay notify.

19. (*1*) The Board shall consist of a Chairperson and such number of other Members as the Central Government may notify.

(2) The Chairperson and other Members shall be appointed by the Central Governmentin such manner as may be prescribed.

(3) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Board, and at least one among them shall be an expert in the field of law.

20. (*1*) The salary, allowances and other terms and conditions of service of the Chairperson and other Members shall be such as may be prescribed, and shall not be varied to their disadvantage after their appointment.

(*2*) The Chairperson and other Members shall hold office for a term of two years and shall be eligible for re-appointment.

21. (*1*) A person shall be disqualified for being appointed and continued as the Chairperson or a Member, if she—

(a) has been adjudged as an insolvent;

(b) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude;

(c) has become physically or mentally incapable of acting as a Member;

(d) has acquired such financial or other interest, as is likely to affect prejudiciallyher functions as a Member; or

(e) has so abused her position as to render her continuance in office prejudicialto the public interest.

(*2*) The Chairperson or Member shall not be removed from her office by the Central Government unless she has been given an opportunity of being heard in the matter.

22. (*1*) The Chairperson or any other Member may give notice in writing to the Central Government of resigning from her office, and such resignation shall be effective from the date on

which the Central Government permits her to relinquish office, or upon expiry of a period of three months from the date of receipt of such notice, or upon a duly appointed successor entering upon her office, or upon the expiry of the term of her office, whichever is earliest.

(2) A vacancy caused by the resignation or removal or death of the Chairperson orany other Member, or otherwise, shall be filled by fresh appointment in accordance with the provisions of this Act.

(3) The Chairperson and any other Member shall not, for a period of one year from thedate on which they cease to hold such office, except with the previous approval of the Central Government, accept any employment, and shall also disclose to the Central Government any subsequent acceptance of employment with any Data Fiduciary against whom proceedings were initiated by or before such Chairperson or other Member.

23. (*1*) The Board shall observe such procedure in regard to the holding of and transaction of business at its meetings, including by digital means, and authenticate its orders, directions and instruments in such manner as may be prescribed.

(2) No act or proceeding of the Board shall be invalid merely by reason of—

(a) any vacancy in or any defect in the constitution of the Board;

(b) any defect in the appointment of a person acting as the Chairperson or otherMember of the Board; or

(c) any irregularity in the procedure of the Board, which does not affect themerits of the case.

(3) When the Chairperson is unable to discharge her functions owing to absence,illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson until the date on which the Chairperson resumes her duties.

24. The Board may, with previous approval of the Central Government, appoint suchofficers and employees as it may deem necessary for the efficient discharge of its functions under the provisions of this Act, on such terms and conditions of appointment and service as may be prescribed.

25. The Chairperson, Members, officers and employees of the Board shall be deemed, when acting or purporting to act in pursuance of provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.

26. The Chairperson shall exercise the following powers, namely:—

a general superintendence and giving direction in respect of all administrative matters of the Board;

b authorise any officer of the Board to scrutinise any intimation, complaint, reference or correspondence addressed to the Board; and

c authorise performance of any of the functions of the Board and conduct any of its proceedings, by an individual Member or groups of Members and to allocate proceedings among them.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CHAPTER VI
POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD

27. (1) The Board shall exercise and perform the following powers and functions, namely:—

a on receipt of an intimation of personal data breach under sub-section (6) of section 8, to direct any urgent remedial or mitigation measures in the event of a personal data breach, and to inquire into such personal data breach and impose penalty as provided in this Act;

b on a complaint made by a Data Principal in respect of a personal data breach or a breach in observance by a Data Fiduciary of its obligations in relation to her personal data or the exercise of her rights under the provisions of this Act, or on a reference made to it by the Central Government or a State Government, or in compliance of the directions of any court, to inquire into such breach and impose penalty as provided in this Act;

c on a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to her personal data, to inquire into such breach and impose penalty as provided in this Act;

d on receipt of an intimation of breach of any condition of registration of a Consent Manager, to inquire into such breach and impose penalty as provided in this Act; and

e on a reference made by the Central Government in respect of the breach in observance of the provisions of sub-section (2) of section 37 by an intermediary, to inquire into such breeach and impose penalty as provided in this Act.

(2) The Board may, for the effective discharge of its functions under the provisions of this Act, after giving the person concerned an opportunity of being heard and after recording reasons in writing, issue such directions as it may consider necessary to such person, who shall be bound to comply with the same.

(3) The Board may, on a representation made to it by a person affected by a direction issued under sub-section (1) or sub-section (2), or on a reference made by the Central Government, modify, suspend, withdraw or cancel such direction and, while doing so, impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

28. (1) The Board shall function as an independent body and shall, as far as practicable, function as a digital office, with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt such techno-legal measures as may be prescribed.

(2) The Board may, on receipt of an intimation or complaint or reference or directionsas referred to in sub-section (*1*) of section 27, take action in accordance with the provisions of this Act and the rules made thereunder.

(3) The Board shall determine whether there are sufficient grounds to proceed with aninquiry.

(4) In case the Board determines that there are insufficient grounds, it may, for reasonsto be recorded in writing, close the proceedings.

(5) In case the Board determines that there are sufficient grounds to proceed withinquiry, it may, for reasons to be recorded in writing, inquire into the affairs of any person for ascertaining whether such person is complying with or has complied with the provisions of this Act.

(6) The Board shall conduct such inquiry following the principles of natural justiceand shall record reasons for its actions during the course of such inquiry.

(7) For the purposes of discharging its functions under this Act, the Board shall have5 of 1908. the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in respect of matters relating to—

(a) summoning and enforcing the attendance of any person and examining heron oath;

(b) receiving evidence of affidavit requiring the discovery and production ofdocuments;

(c) inspecting any data, book, document, register, books of account or anyother document; and

(d) such other matters as may be prescribed.

(8) The Board or its officers shall not prevent access to any premises or take intocustody any equipment or any item that may adversely affect the day-to-day functioning of a person.

(9) The Board may require the services of any police officer or any officer of theCentral Government or a State Government to assist it for the purposes of this section and it shall be the duty of every such officer to comply with such requisition.

(10) During the course of the inquiry, if the Board considers it necessary, it may forreasons to be recorded in writing, issue interim orders after giving the person concerned an opportunity of being heard.

(11) On completion of the inquiry and after giving the person concerned an opportunityof being heard, the Board may for reasons to be recorded in writing, either close the proceedings or proceed in accordance with section 33.

(12) At any stage after receipt of a complaint, if the Board is of the opinion that thecomplaint is false or frivolous, it may issue a warning or impose costs on the complainant.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CHAPTER VII
APPEAL AND ALTERNATE DISPUTE RESOLUTION

29. (*1*) Any person aggrieved by an order or direction made by the Board under this Act may prefer an appeal before the Appellate Tribunal.

(2) Every appeal under sub-section (*1*) shall be filed within a period of sixty days from the date of receipt of the order or direction appealed against and it shall be in such form and manner and shall be accompanied by such fee as may be prescribed.

(3) The Appellate Tribunal may entertain an appeal after the expiry of the periodspecified in sub-section (*2*), if it is satisfied that there was sufficient cause for not preferring the appeal within that period.

(4) On receipt of an appeal under sub-section (*1*), the Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Appellate Tribunal shall send a copy of every order made by it to the Boardand to the parties to the appeal.

(6) The appeal filed before the Appellate Tribunal under sub-section (*1*) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date on which the appeal is presented to it.

(7) Where any appeal under sub-section (*6*) could not be disposed of within the period of six months, the Appellate Tribunal shall record its reasons in writing for not disposing of the appeal within that period.

(8) Without prejudice to the provisions of section 14A and section 16 of the Telecom Regulatory Authority of India Act, 1997, the Appellate Tribunal shall deal with an appeal under this section in accordance with such procedure as may be prescribed.

(9) Where an appeal is filed against the orders of the Appellate Tribunal under thisAct, the provisions of section 18 of the Telecom Regulatory Authority of India Act, 1997 shall apply.

(10) In respect of appeals filed under the provisions of this Act, the Appellate Tribunalshall, as far as practicable, function as a digital office, with the receipt of appeal, hearing and pronouncement of decisions in respect of the same being digital by design.

30. (*1*) An order passed by the Appellate Tribunal under this Act shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(*2*) Notwithstanding anything contained in sub-section (*1*), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

31. If the Board is of the opinion that any complaint may be resolved by mediation, it may direct the parties concerned to attempt resolution of the dispute through such mediation by such mediator as the parties may mutually agree upon, or as provided for under any law for the time being in force in India.

32. (*1*) The Board may accept a voluntary undertaking in respect of any matter related to observance of the provisions of this Act from any person at any stage of a proceeding under section 28.

(2) The voluntary undertaking referred to in sub-section (*1*) may include an undertaking to take such action within such time as may be determined by the Board, or refrain from taking such action, and or publicising such undertaking.

(3) The Board may, after accepting the voluntary undertaking and with the consent ofthe person who gave the voluntary undertaking vary the terms included in the voluntary undertaking.

(4) The acceptance of the voluntary undertaking by the Board shall constitute a baron proceedings under the provisions of this Act as regards the contents of the voluntary undertaking, except in cases covered by sub-section (*5*).

(5) Where a person fails to adhere to any term of the voluntary undertaking acceptedby the Board, such breach shall be deemed to be breach of the provisions of this Act and the Board may, after giving such person an opportunity of being heard, proceed in accordance with the provisions of section 33.

CHAPTER VIII
PENALTIES AND ADJUDICATION

33. (*1*) If the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may, after giving the person an opportunity of being heard, impose such monetary penalty specified in the Schedule.

(*2*) While determining the amount of monetary penalty to be imposed under sub-section (*1*), the Board shall have regard to the following matters, namely:—

(a) the nature, gravity and duration of the breach;

(b) the type and nature of the personal data affected by the breach;

(c) repetitive nature of the breach;

(d) whether the person, as a result of the breach, has realised a gain or avoidedany loss;

(e) whether the person took any action to mitigate the effects and consequencesof the breach, and the timeliness and effectiveness of such action;

(f) whether the monetary penalty to be imposed is proportionate and effective,having regard to the need to secure observance of and deter breach of the provisions of this Act; and

(g) the likely impact of the imposition of the monetary penalty on the person.

34. All sums realised by way of penalties imposed by the Board under this Act, shall be credited to the Consolidated Fund of India.

CHAPTER IX
MISCELLANEOUS

35. No suit, prosecution or other legal proceedings shall lie against the Central Government, the Board, its Chairperson and any Member, officer or employee thereof for anything which is done or intended to be done in good faith under the provisions of this Act or the rules made thereunder.

36. The Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for.

37. (*1*) The Central Government or any of its officers specially authorised by it in this behalf may, upon receipt of a reference in writing from the Board that—

(a) intimates the imposition of monetary penalty by the Board on a Data Fiduciaryin two or more instances; and

(b) advises, in the interests of the general public, the blocking for access by thepublic to any information generated, transmitted, received, stored or hosted, in any computer resource that enables such Data Fiduciary to carry on any activity relating to offering of goods or services to Data Principals within the territory of India, after giving an opportunity of being heard to that Data Fiduciary, on being satisfied that it is necessary or expedient so to do, in the interests of the general public, for reasons to be recorded in writing, by order, direct any agency of the Central Government or any intermediary to block for access by the public or cause to be blocked for access by the public any such information.

(2) Every intermediary who receives a direction issued under sub-section (*1*) shall be bound to comply with the same.

(3) For the purposes of this section, the expressions “computer resource”, “information” and “intermediary” shall have the meanings respectively assigned to them in the Information Technology Act, 2000.

38. (*1*) The provisions of this Act shall be in addition to and not in derogation of any other law for the time being in force.

(*2*) In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict.

39. No civil court shall have the jurisdiction to entertain any suit or proceeding in respect of any matter for which the Board is empowered under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power under the provisions of this Act.

40. (*1*) The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act.

(*2*) In particular and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(a)the manner in which the notice given by the Data Fiduciary to a Data Principalshall inform her, under sub-section (*1*) of section 5;

(b) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (*2*) of section 5;

(c)the manner of accountability and the obligations of Consent Manager undersub-section (*8*) of section 6;

(d) the manner of registration of Consent Manager and the conditions relatingthereto, under sub-section (*9*) of section 6;

(e)the subsidy, benefit, service, certificate, licence or permit for the provision orissuance of which, personal data may be processed under clause (*b*) of section 7;

(f) the form and manner of intimation of personal data breach to the Board undersub-section (*6*) of section 8;

(g) the time period for the specified purpose to be deemed as no longer being served, under sub-section (*8*) of section 8;

(h) the manner of publishing the business contact information of a DataProtection Officer under sub-section (*9*) of section 8;

(i) the manner of obtaining verifiable consent under sub-section (*1*) of section 9;

(j) the classes of Data Fiduciaries, the purposes of processing of personal dataof a child and the conditions relating thereto, under sub-section (*4*) of section 9;

(k) the other matters comprising the process of Data Protection ImpactAssessment under sub-clause (*i*) of clause (*c*) of sub-section (*2*) of section 10;

(l) the other measures that the Significant Data Fiduciary shall undertake undersub-clause (*iii*) of clause (*c*) of sub-section (*2*) of section 10;

(m) the manner in which a Data Principal shall make a request to the DataFiduciary to obtain information and any other information related to the personal data of such Data Principal and its processing, under sub-section (*1*) of section 11;

(n) the manner in which a Data Principal shall make a request to the DataFiduciary for erasure of her personal data under sub-section (*3*) of section 12;

(o) the period within which the Data Fiduciary shall respond to any grievancesunder sub-section (*2*) of section 13;

(p) the manner of nomination of any other individual by the Data Principalunder sub-section (*1*) of section 14;

(q) the standards for processing the personal data for exemption under clause (*b*) of sub-section (*2*) of section 17;

(r) the manner of appointment of the Chairperson and other Members of theBoard under sub-section (*2*) of section 19;

(s) the salary, allowances and other terms and conditions of services of theChairperson and other Members of the Board under sub-section (*1*) of section 20;

(t) the manner of authentication of orders, directions and instruments undersub-section (*1*) of section 23;

(u) the terms and conditions of appointment and service of officers andemployees of the Board under section 24;

(v) the techno-legal measures to be adopted by the Board under sub-section (*1*) of section 28;

(w) the other matters under clause (*d*) of sub-section (*7*) of section 28;

(x) the form, manner and fee for filing an appeal under sub-section (*2*) of section 29;

(y) the procedure for dealing an appeal under sub-section (*8*) of section 29;

(z) any other matter which is to be or may be prescribed or in respect of whichprovision is to be, or may be, made by rules.

41. Every rule made and every notification issued under section 16 and section 42 of this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if before the

expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or notification or both Houses agree that the rule or notification should not be made or issued, the rule or notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or notification.

Power to

42. (*1*) The Central Government may, by notification, amend the Schedule, subject to the restriction that no such notification shall have the effect of increasing any penalty specified therein to more than twice of what was specified in it when this Act was originally enacted.

(*2*) Any amendment notified under sub-section (*1*) shall have effect as if enacted in this Act and shall come into force on the date of the notification.

43. (*1*) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to it to be necessary or expedient for removing the difficulty.

(2) No order as referred to in sub-section (*1*) shall be made after the expiry of three years from the date of commencement of this Act.

(3) Every order made under this section shall be laid, as soon as may be after it ismade, before each House of Parliament.

44. (*1*) In section 14 of the Telecom Regulatory Authority of India Act, 1997, in clause (*c*), for sub-clauses (*i*) and (*ii*), the following sub-clauses shall be substituted, namely:—

"(*i*) the Appellate Tribunal under the Information Technology Act, 2000;

(ii) the Appellate Tribunal under the Airports Economic Regulatory Authority of India Act, 2008; and

(iii) the Appellate Tribunal under the Digital Personal Data ProtectionAct, 2023.".

(2) The Information Technology Act, 2000 shall be amended in the following manner,namely:—

(a) section 43A shall be omitted;

(b) in section 81, in the proviso, after the words and figures "the PatentsAct, 1970", the words and figures "or the Digital Personal Data Protection Act, 2023" shall be inserted; and

(c) in section 87, in sub-section (*2*), clause (*ob*) shall be omitted.

(3) In section 8 of the Right to Information Act, 2005, in sub-section (*1*), for clause (*j*), the following clause shall be substituted, namely:—

"(*j*) information which relates to personal information;".

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

THE SCHEDULE

[*See* section 33 (*1*)]

Sl. No.	Breach of provisions of this Act or rules made thereunder	Penalty
(1)	(2)	(3)

DR. REETA VASISHTA,

Secretary to the Govt. of India