BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 10 N° 5 MARCH 2024

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

Data Protection and Cross-border Data Flows in India

Version 2.0

By Smriti Parsheera

Contents

Executive Summary

Following a long drawn deliberation process, India recently adopted its first comprehensive data protection law in 2023. The Digital Personal Data Protection Act, 2023 (DPD Act, 2023), which is expected to come into effect during this year, differs from other global data protection frameworks in some respects. For instance, it applies only to data that is collected or processed in a digital form, it does not create a separate category of sensitive personal data, and does not entitle individuals to seek compensation from data fiduciaries for any harms caused to them. Further, the law is also silent on some of the other aspects that are seen in laws like the European GDPR. For instance, the rights related to data portability, the right to be forgotten, and automated decision-making. However, the government has indicated that some of these aspects may be covered under a future companion legislation to the DPD Act, known as the proposed Digital India Act.

The treatment of cross-border data flows is another point of divergence. The position adopted by the Indian law is that personal data will be allowed to flow freely, except to a set of restricted countries that can be notified by the government. This represents a significant shift from the initial drafts of the law, which proposed strict localization requirements for certain types of data and identified mechanisms like adequacy assessments, model contract clauses and intra-group schemes as conditional modes of data transfers.

While the new law has settled on a fairly liberal stance toward personal data flows, it leaves the door open for the adoption of more stringent restrictions under other laws. India already has a number of such sector/ data-type related transfer restrictions that are applicable to the financial sector, telecommunication and broadcasting services, corporate and compliance requirements, and government data.

Set against this background, Section 1 of the paper begins with a discussion on India's key data governance initiatives and priorities, much of which has been centered around the role of data for effective governance, innovation and empowerment. It highlights the role of digital public infrastructure solutions like the Data Empowerment and Protection Architecture and the proposed National Data Management Office in the country's data governance strategy.

Section 2 describes the evolution of India's data protection framework, with a focus on the scope, rights and obligations and enforcement mechanisms under the DPD Act, 2023. This is followed, in Section 3, with a deep dive into the cross-border flow related provisions. The section describes the transition from the localization recommendations of 2018 to the blacklisting approach under the DPD Act. It then maps out the different sector-specific restrictions that exist in India and explores the country's position on data sharing and data flows under international arrangements.

Section 4 presents an analysis of the key issues that emerge from the discussions and offers some recommendations. Rather than making broader suggestions on general improvements that may be needed to the DPD Act, the paper limits itself to recommendations on issues related to cross border data flow.

First, it recommends that, in order to minimize fragmentation and uncertainty, the law should set out the basic principles, criteria, and processes to govern the adoption of any sectoral data flow restrictions. The government's power to impose restrictions on data flows to specific countries should also be bound by such reasonable and identified criteria.

Second, it suggests that stakeholders from the industry can voluntarily take up the initiative of developing model/ standard clauses that would meet the requirements of the DPD Act, and ideally go beyond that, through an open and consultative process. This can serve as a mechanism for building trust among data fiduciaries and processors and facilitating the ease of regulatory compliance.

Third, the paper makes a case for legislative reforms to strengthen the country's surveillance and law enforcement framework. Besides being violative of citizens' privacy rights, unchecked powers of law

enforcement and intelligence agencies are also detrimental to the free flow of data into the country. The suggested reforms would include the introduction of requirements of judicial approval for interception requests, notice to individuals, data minimization requirements, and suitable redress mechanisms.

1 Setting the context

With a population of over 1.4 billion India is now the most populous country in the world.[1] It is the fifth largest economy globally, based on Gross Domestic Product (GDP)[2]. As a lower-middle income country with a rapidly growing economy, India also straddles multiple trade and strategic relationships. It counts the United States (US), China, and the United Arab Emirates (UAE) among its largest trading partners.[3] The country is also known for its leadership in information technology (IT) and business process management services. It holds over fifty percent of the global outsourcing market, with the US, the European Union and the United Kingdom as its largest importers.[4]

In terms of intergovernmental partnerships, India is a member of the Group of Twenty (G20) alliance among the world's largest economies, the Quad diplomatic partnership with Australia, Japan, and the United States, and is recognized as a key partner by the OECD. At the same time, it also prioritizes south-south collaborations through forums like the BRICS forum and the Group of 77 alliance of developing countries.

Despite persisting digital divides, India hosts the world's second largest Internet user base of more than 890 million Internet subscriptions.[5] The foundation of India's digital society rests on the strength of this digital population. Bringing more people online and encouraging their adoption of digital goods and services has, therefore, been a focus for the government and the private sector alike. Correspondingly, the commercial and developmental value of the data generated from such digital interactions has also been in the spotlight.

A large part of the data-related discourse in India is powered by the idea of data being a valuable resource that needs to be harnessed to meet the country's economic and developmental objectives. This includes highlighting the role of data for effective governance and innovation and as a source of citizen empowerment.[6] For instance, India's Economic Survey of 2018-2019 contained a chapter on

---

[1] Laura Silver, Chrustine Huang and Laura Clancy, Key facts as India surpasses China as the world's most populous country, Pew Research (9 February 2023) <https://www.pewresearch.org/short-reads/2023/02/09/key-facts-as-india-surpasses-china-as-the-worlds-most-populous-country/>.

[2] World Bank national accounts data (2022) <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true>;

[3] World Integrated Trade Solution, Top 5 Import and Export Partners (2021) <https://wits.worldbank.org/CountryProfile/en/Country/IND/Year/2021/Summary>. Also see Fazal Rahim, India's foreign trade in 2023: Its top trading partners and most traded commodities, Forbes India (29 December 2023) <https://www.forbesindia.com/article/news/indias-foreign-trade-in-2023-its-top-trading-partners-and-most-traded-commodities/90611/1>.

[4] India Brand Equity Foundation, Servies: Services exports from India stood at US$ 322.72 million in FY23 (November 2023) <https://www.ibef.org/exports/services-industry-india>.

[5] Telecom Regulatory Authority of India, 'The Indian Telecom Services Performance Indicators April–June, 2023' (5 December, 2023) <https://www.trai.gov.in/sites/default/files/QPIR_05122023_0.pdf> accessed 29 January 2024.

[6] Ministry of Electronics and Information Technology, National Data Governance Framework Policy (Draft) (May 2022) <https://www.meity.gov.in/writereaddata/files/National%20Data%20Governance%20Framework%20Policy_26%20May%202022.pdf>.

"Data 'Of the People, By the People, For the People'".[7] The report focused on the different types of data that the government holds about citizens –administrative, survey, institutional and transactions data– and the need to streamline, interlink and unlock this data for public good. Researchers have also identified the role of the government as a market architect and the narrative around countering 'data colonialism' as some of the other drivers behind India's data governance strategy.[8]

The country's reliance on digital public infrastructure (DPI), as the predominant path to digital transformation,[9] has also influenced its data governance solutions. Two examples of such data governance-centric DPIs, which emphasize the importance of digital infrastructures for improved data gathering, storage, processing and dissemination, are currently in motion. The first, the Data Empowerment and Protection Architecture (DEPA), is a technical architecture designed to facilitate the sharing of personal data among entities, relying on an electronic consent artifact.[10] This artifact would record the individual's consent for the sharing of their data held by one entity, such as a diagnostic lab, with another entity, such as a hospital. In the financial sector, DEPA has been implemented under the regulatory framework governing a new category of intermediaries called 'account aggregators'.[11] These entities act on the user's consent to facilitate the flow of encrypted information among financial institutions through the use of application programming interfaces (APIs).

The second initiative relates to the move toward the creation of a 'India Data Management Office' (IDMO) that was introduced in the draft National Data Governance Framework Policy released in 2022.[12] The proposed IDMO will be responsible for developing rules and standards to govern the collection, management and exchange of non-personal and anonymized data generated by government entities. Private entities would also be encouraged to contribute to its datasets generation program and a subset of them (specifically, only India-based entities) would also be allowed access to the datasets. The final version of this policy is yet to be notified.[13]

Besides such technical architectures for data management, India has launched a number of policy deliberations pertaining to data governance. Notable among these are the enactment of the Digital Personal Data Protection Act, 2023 (DPD Act), which is discussed further in Section 2, and a proposal for the regulation and sharing of non personal data. In 2019, the Indian government set up a committee of experts on non-personal data. The committee recommended the need for a new regulatory framework for unlocking the economic benefit of non-personal data that is generated in India and

---

[7] Economic Survey of 2018-2019, Data "Of the People, By the People, For the People" <https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04_vol1.pdf>

[8] Neha Mishra, Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?, in Data Sovereignty: From the Digital Silk Road to the Return of the State, Anupam Chander and Haochen Sun (eds.) (New York, 2023; online edn, Oxford Academic, 14 December 2023) <https://doi.org/10.1093/oso/9780197582794.003.0011>.

[9] 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>.

[10] NITI Aayog, 'Data Empowerment and Protection Architecture: Draft for Discussion' (2020) <https://www.niti.gov.in/sites/default/ files/2020-09/DEPA-Book.pdf>; Draft Report by the Committee of Experts on Non-Personal Data Governance Framework (16 December 2020) <https://static.mygov.in/static/s3fs-public/mygov_160975438978977151.pdf> accessed 2 February 2024.

[11] Press Information Bureau, Know all about Account Aggregator Network – A financial data-sharing system (September 2021) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713>.

[12] Ministry of Electronics and Information Technology (n 6).

[13] Gargi Sarkar, Draft National Data Governance Policy Under Finalisation: Centre, Inc42 (1 February 2024) <https://inc42.com/buzz/draft-national-data-governance-policy-under-finalisation-centre/>.

should be available to meet the country' governance and innovation goals.[14] Unlike the IDMO initiative, which concentrates primarily on government-owned data, the committee recommended that even private businesses should be compelled to create and share 'high value datasets' for certain public good purposes.[15] The government is yet to take a final decision on the committee's recommendations although the proposed IDMO might be a precursor to such a move.

The issue of cross border data flows has featured prominently in many of these regulatory discussions. Notably so, in the case of the data protection law, which went through many draft versions until its final enactment in 2023. These draft versions of the text contained varying levels of data flow restrictions, starting from the proposal for mandatory mirroring of all personal data on Indian servers in the first draft of 2018 to the significantly relaxed approach adopted in the enacted version. Section 3 of the paper describes the progression of these ideas as well as the interplay between the data protection law and various sector-specific data flow restrictions that will continue to remain in effect.

The Indian government is in the process of formulating another law, the proposed Digital India Act, which it describes as a 'companion legislation' to the DPD Act.[16] While a draft of this has not yet been published, an early consultation document indicates that the proposed law will cover various aspects of digital user rights, including the right to be forgotten, right to redress, and right against discrimination and automated decision making.[17] The manner in which the provisions of the DPD Act will interact with the proposed Digital India Act is not yet clear.

At present, India is not pursuing an independent legislation to regulate artificial intelligence, although some aspects of this will be covered under the Digital India Act. Its official think tank, the NITI Aayog has, however, formulated a national AI strategy document[18] and the government has issued various advisories on the subject. For instance, the advisory directed at significant social media intermediaries to identify misinformation and deepfakes.[19] More recently, the government introduced, and then hastily backtracked on, another controversial advisory that advised the need for taking its permission before deploying 'unreliable' AI models.[20]

---

[14] Committee of Experts on Non-Personal Data Governance Framework (n 10).

[15] The indicated list of public purposes would include improving public services, agriculture, healthcare, job creation, poverty alleviation and financial inclusion.

[16] Ministry of Electronics and Information Technology, Digital Personal Data Protection Act is a world-class legislation: MoS Rajeev Chandrasekhar (13 August 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357>.

[17] Ministry of Electronics and Information Technology, Proposed Digital India Act, 2023, Digital India Dialogues (9 March 2023) <https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf>.

[18] NITI Aayog, National Strategy for Artificial Intelligence (June 2018) <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>.

[19] Ministry of Electronics and Information Technology, Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes (7 November 2023) <https://pib.gov.in/PressReleasePage.aspx?PRID=1975445>.

[20] Amber Sinha, The Many Questions About India's New AI Advisory, Tech Policy Press (6 March 2024) <https://www.techpolicy.press/the-many-questions-about-indias-new-ai-advisory/>; Paritosh Chauhan, Sameer Avasarala and Abhishek Singh, MEITY Advisory: Dawn of AI Regulation in India or a false start, Lexology (1 April 2024) <https://www.lexology.com/library/detail.aspx?g=47dda3b5-1111-4b6b-9f87-799ef8066802>.

2 Legal framework on data protection

India is a recent entrant into the club of jurisdictions with comprehensive data protection laws. Its DPD Act was approved by both houses of the Parliament and received the President's assent in August 2023. The new law is, however, yet to come into effect. The Ministry of Electronics and Information Technology (MeitY), the ministry in charge of this subject, is likely to start notifying different provisions post the conclusion of India's general elections in June 2024.[21] Meanwhile, the MeitY is reported to be in the process of developing the draft rules needed to operationalize various aspects of the new law.[22]

Until the DPD Act is brought into effect, data protection issues continue to be governed mainly under the limited set of protections offered under Section 43A and 72A of the Information Technology Act, 2000. Section 43A of this law provides for compensation in case a body corporate fails to maintain reasonable security practices while dealing with sensitive personal data. Section 72A lays down criminal penalties for unauthorized disclosure of personal data. The government has also framed a set of rules governing the processing and security of sensitive personal data under Section 43A.[23] Among other provisions, the rules lay down requirements related to data transfers, providing that a transfer should be made only if it is necessary for the performance of a lawful contract or with the individual's consent.[24] Further, the parties to the transfer will be bound to ensure that the data remains subject to the same level of data protection as set out under the rules for the body corporate collecting the data.[25] Upon the implementation of the DPD Act, the data flow conditions under these rules will be replaced by the relatively less restrictive framework for cross-border data flows under the new law.

2.1 Evolution of the data protection law

Policy discussions on the need for a standalone privacy law had been going on in India since 2010,[26] but the process did not see much traction until a few years ago. In August 2017, a nine-judge bench of the Supreme Court examined the issue of whether the Indian Constitution guarantees a fundamental right to privacy. Answering the question in the affirmative, the court in Justice KS Puttaswamy and another v. Union of India[27] laid down that privacy is a fundamental right, although not an absolute one. The judges held that any reasonable intrusion into the right to privacy would be valid only if it

[21] Ashmit Kumar, Data Protection Framework postponed until after Lok Sabha elections: Sources, CNBC TV18 (17 January 2024) <https://www.cnbctv18.com/technology/data-protection-framework-postponed-dpdp-notifcation-after-lok-sabha-elections-18823331.htm>.

[22] Aditi Agrawal, Draft rules on data protection to be shared this week: MoS Chandrasekhar, The Hindustan Times (21 December 2023) <https://www.hindustantimes.com/india-news/draft-rules-on-data-protection-to-be-shared-this-week-mos-chandrasekhar-101703159717469.html>.

[23] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 <https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf>.

[24] Rule 7, Information Technology Rules, 2011.

[25] This includes requirements relating to maintaining reasonable security practices and not retaining the information for longer than is required for the original, lawful, purpose.

[26] Ministry of Personnel, Approach paper for a legislation on privacy (Draft) (13 October 2010) <https://documents.doptcirculars.nic.in/D2/D02rti/aproach_paper.pdf>. Also see Malavika Raghavan, Are we there yet? The long road to nowhere: The demise of India's draft data protection bill, Future of Privacy Forum (October 2022) <https://fpf.org/blog/are-we-there-yet-the-long-road-to-nowhere-the-demise-of-indias-draft-data-protection-bill/>.

[27] Justice KS Puttaswamy and another v. Union of India, Writ Petition (Civil) No. 494 of 2012 <https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf>

satisfies the tests of legality, legitimate aim, and proportionality. Such an intervention must also incorporate reasonable procedural safeguards.[28]

Further, a plurality of the judges in the Puttaswamy decision recognized that the right to privacy consists of many different facets, informational privacy being one of them. They observed that data protection is a complex exercise which needs to be undertaken by the state after a careful balancing of the requirements of privacy coupled with other values and the state's legitimate concerns.[29] In the lead up to this verdict, the Indian government set up an expert committee to study the issues relating to data protection in India and recommend a draft data protection bill. The committee, headed by a former Supreme Court judge, Justice B.N. Srikrishna, identified the need to develop a legal framework that would speak to India's priorities as a developing nation while also drawing upon the best practices of data protection in more developed democracies.[30] As per several accounts, the committee's Draft Data Protection Bill of 2018[31] ended up drawing significant inspiration from the European General Data Protection Regulation (GDPR). Yet, it also left room for improvements in order to be better tuned to the Indian context.[32]

Following public consultations, the MeitY generated a revised version of the bill, which was introduced in Parliament as the Personal Data Protection Bill of 2019.[33] A Joint Parliamentary Committee (JPC), consisting of members from both houses of the Indian Parliament, was then tasked to review the bill and offer their recommendations on it. The JPC recommended that the scope of the bill should explicitly cover both personal and non-personal data, including anonymized personal data.[34] The committee also suggested other edits to increase the scope of harms under the law, impose stricter regulations on social media intermediaries, and regulate data-collecting hardware manufacturers. However, in 2022, the government announced its decision to withdraw the pending bill and subsequently replaced it with a new draft. This revised draft of 2022 is the one that eventually made it to the rule book as the DPD Act.

---

[28] Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman, An analysis of Puttaswamy: the Supreme Court's privacy verdict, The LEAP Blog (20 September 2017) <https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html#gsc.tab=0>.

[29] Chandrachud J. in Justice KS Puttaswamy and another v. Union of India, para 179, p. 253.

[30] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, '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 30 January 2024.

[31] The Personal Data Protection Bill, 2018 <https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>

[32] Nilesh Christopher, Srikrishna Committee Report: Draft bill gets mixed response from experts, The Economic Times (28 July 2018) <https://economictimes.indiatimes.com/news/politics-and-nation/srikrishna-committee-report-draft-bill-gets-mixed-response-from-experts/articleshow/65171992.cms?from=mdr>; Raman Jit Singh Chima, Naman M. Aggarwal and Akash Singh, India's Draft Data Protection Bill Needs to do More to Stack Up Against Global Standards, The Wire (25 September 2018) <https://thewire.in/tech/data-protection-bill-supreme-court-puttaswamy-judgment>.

[33] The Personal Data Protection Bill, 2019 <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf>

[34] Report of the Joint Committee on Personal Data Protection Bill, 2019, Lok Sabha Secretariat (2021) <https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf>.

2.2 Scope of the DPD Act

The DPD Act will govern the processing of all digital personal data – data that is collected in a digital form or digitized post collection– that takes place in India. It will also have extraterritorial scope over processing that takes place outside India but is connected with a business or systematic activity of offering goods or services to, or the profiling of, persons in India.[35] In terms of nomenclature, starting from Justice Srikrishna committee's draft bill in 2018, India has used the terms 'data principal' and 'data fiduciary' to identify what the European GDPR would call the 'data subject' and 'data controller'. In the committee's view, the term principal was better suited to capture the individual's role as 'the focal actor in the digital economy' while the concept of fiduciary was invoked to imply a duty of care to deal with the individual's data fairly and responsibly.[36] Researchers observed that the scope of duties and the standards laid down in the committee's draft law, which have only been diluted over time, were not as high as seen in cases of traditional fiduciary relationships like doctor-patient and lawyer-client.[37] But it remains to be seen if the implementation of the DPD Act could result in the development of a new body specific to the processing of personal data.[38]Next, the law contains several exclusions and exemptions from its scope. To begin with, the DPD Act will not apply to any processing done by an individual for personal or domestic purposes. Any data that is made publicly available by the relevant data principal, such as on social media, or by any other person under a legal obligation is also excluded.[39] Further, the law also excludes any processing done for research, archiving or statistical purposes so long as no specific decision is being made about the data principal and such processing adhered with prescribed standards.[40] The scope of what is covered under the meaning of 'research' has not been laid down in the law and will likely be clarified in the standards to be prescribed by the government for this purpose.

Further, there are two other categories of exemptions. The first relates to exemptions from an albeit broad, but identified, set of provisions for purposes like judicial or regulatory, law enforcement, giving effect to a merger or amalgamation, and default in loan payment.[41] The second group covers those cases where the power to notify the exemption is vested in the hands of the government. For instance, the power to exempt state instrumentalities for national interest or public order objectives or Indian startups and other select fiduciaries to ease their compliance burden.[42] In addition, there is an open-ended power for the government to declare, within the first five years, that any provision of the law will not apply to any fiduciary(ies) for a notified period.[43]

[35] Section 3(a) and (b), DPD Act 2023.
[36] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 30), p. 8.
[37] Rishab Bailey and Trishee Goyal, Fiduciary Relationships as a Means to Protect Privacy: Examining the Use of the Fiduciary Concept in the Draft Personal Data Protection Bill, 2019' (The Leap Blog, 13 January 2020) <https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html>
[38] Smitha Krishna Prasad, Information Fiduciaries and India's Data Protection Law, Data Catalyst (September 2019) <https://datacatalyst.org/wp-content/uploads/2020/06/Information-Fiduciaries-and-Indias-Data-Protection-Law.pdf>.
[39] Section 3(c), DPD Act 2023.
[40] Section 17(2)(b), DPD Act 2023.
[41] Section 17(1), DPD Act 2023.
[42] Section 17(2)(a) and 17(3), DPD Act 2023.
[43] Section 17(5), DPD Act 2023.

2.3 Rights and obligations

The processing of personal data can take place either based on the consent of the data principal or under any of the specified 'legitimate uses'. The list of legitimate grounds includes voluntary provision of data to the data fiduciary, which is not accompanied by a denial of consent for its processing, provision of services and benefits by the state, disasters and medical emergencies.[44] Further, data processing for employment-related purposes and to protect the employer from incidents of corporate espionage or intellectual property breach is also classified as a legitimate use.

In situations where the data processing is based on consent, the law provides for a requirement of notice about the purpose of the processing and the manner in which the individual can exercise their rights. Taking into account the diversity of the Indian population, the law requires that the individual should be given the option to access any request for in English or any of the twenty two Indian languages specified in the Constitution.[45] However, unlike many other data protection laws, the DPD Act does not recognize a separate category of sensitive personal data that may merit higher safeguards for notice and consent or for any other purposes. This also stands in contrast with the position under IT Act and rules, which applied specifically to sensitive personal data.

There is a list of general obligations that have been cast on data fiduciaries.[46] This includes ensuring the completeness and accuracy of data, reasonable security safeguards to prevent a data breach, erasure of personal data, and an effective mechanism for grievance redress. Further, the processing of childrens' data is subject to requirements of verifiable parental consent and restrictions on tracking, behavioral monitoring and targeted advertising aimed at children.[47] In addition to these general requirements, an additional set of obligations, including conduct of impact assessments and external data audits, will apply only to 'significant data fiduciaries' to be notified by the government.[48]

The DPD Act also grants four categories of rights to data principals. In case of consent based processing, the person is entitled to seek a summary of their processed data and identities of others with whom the data has been shared.[49] Similarly, the right to correction and erasure of data is also limited to consensual processing.[50] The two other rights – that of access to grievance redress and the right to appoint a nominee to deal with a person's data upon their death or incapacity – will apply in all cases.[51] While conferring these rights, the law casts a set of expected duties from the data principal, such as not suppressing any material information and not filing false or frivolous complaints.[52]

2.4 Enforcement framework

The DPD Act provides for the creation of a new statutory body called the Data Protection Board of India (the Board) to inquire into compliance with the provisions of the law. The Board's functions will also include directing remedial or mitigation measures against any data breach, checking compliance by consent management intermediaries registered under the DPD Act.[53] While the text

[44] Section 7, DPD Act.
[45] Sections 5 and 6, DPD Act 2023.
[46] Section 8, DPD Act 2023.
[47] Section 9, DPD Act 2023.
[48] Section 10, DPD Act 2023.
[49] Section 11, DPD Act 2023
[50] Section 12, DPD Act 2023.
[51] Section 13 and 14, DPD Act, 2023.
[52] Section 15, DPD Act 2023.
[53] Section 27, DPD Act 2023.

of the law states that the Board will function as an independent body,[54] commentators have called into question the extent of this independence in light of the significant government control over the membership and functioning of the Board.[55]

Pursuant to conducting an inquiry, the Board may impose monetary penalties up to the limits specified in the law for different types of actions. While doing so, it should take into account facts like the nature and gravity of the breach, its repetitive nature and existence of any mitigating actions. The maximum penalty specified in the Schedule stands at Indian Rupees 2.5 billion (approximately 27.5 million Euros). An appeal against the order of the Board can be made to an Appellate Tribunal designated under the law. Notably, there is no provision for the payment of compensation to data principals for harms caused to them by a data fiduciary or processor. This is unlike the provisions seen in laws like the GDPR or the right to compensation under Section 43A of the IT Act, which will no longer remain in effect.

Departing from earlier drafts of the bill, the DPD Act also does not confer any regulation-making powers on the Board.[56] It, however, identifies several areas for rule-making by the central government. The list of powers in Section 40 includes the manner of issuance of notice, exemptions related to processing of children's data, and the process of conducting data protection impact assessments. In addition, the government also has the power to issue notifications on several important subjects, including cross border data flows, which is discussed in the next section. Further, the government can, based on a reference received from the Board, issue directions for the blocking of the business activities of an entity upon which a monetary penalty has already been imposed in two or more instances.[57]

2.5 Data access for surveillance and law enforcement

The broad exemptions afforded by the DPD Act for law enforcement and other designated purposes come against the background of a deficient framework of surveillance-related protections under other laws.[58] The interception of telecommunications messages and information on a computer resource is governed by Section 69 of the Information Technology Act, 2000 and Section 20(2) of the Telecommunications Act 2023 (previously Section 5(2) of the Telegraph Act, 1885). These provisions allow for the government to call for the interception and disclosures of messages to the government on grounds such as the sovereignty and integrity of the nation, defense and state security, public order, or preventing the incitement of any offense.

[54] Section 28, DPD Act 2023.

[55] Aarathi Ganesan, Will the Composition of the Data Protection Board of India Impact How it Handles Data Privacy Complaints?, Medianama (2 November 2023) <https://www.medianama.com/2023/11/223-composition-data-protection-board-impact/>; Gargi Sarkar, Experts Raise Questions On The Autonomy Of The Proposed Data Protection Board, Inc42 (25 November 2022 <https://inc42.com/buzz/autonomy-of-the-proposed-data-protection-board-is-in-question-experts/>.

[56] Anirudh Burman, Understanding India's New Data Protection Law, Carnegie India (3 October 2023) <https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624>.

[57] Section 37, DPD Act 2023.

[58] Jhalak M. Kakkar et al, The Surveillance Law Landscape in India and The Impact of Puttaswamy, National Law University Delhi, Centre for Communication Governance (June 2023) <https://globalnetworkinitiative.org/wp-content/uploads/2023/07/CCG-June-15.pdf>

Following a Supreme Court decision in 1997,[59] the government adopted a set of rules, which were outlined by the court, to govern its interception procedures.[60] The rules designate a senior government official as the person authorized to issue interception orders. However, such orders are not required to be sanctioned by a judicial authority. The only available form of oversight is in the form of a review committee, also consisting of members from the executive, that is supposed to meet at least every two months to review interception orders. There are a few other safeguards like the requirement that such orders should be issued 'only when it is not possible to acquire the information by any other reasonable means'[61] and a prohibition on the use or disclosure of the intercepted messages for any other purpose.[62] The provisions, however, remain silent on other important aspects like independent oversight, notice to the affected person, and transparency and reporting obligations of law enforcement agencies.

Besides the provisions on lawful interception, access to personal data can also be obtained under other laws. Notably, Section 91 of the Code of Criminal Procedure, 1973 contains a broad power enabling an officer in charge of a police station to compel the production of 'any document or other thing' if that is 'necessary or desirable' for the purposes of an investigation. For instance, this power can potentially be used by the police to seek the call data records or SMS logs of an individual, although there have been a handful of cases where courts have stepped in to hold that a blanket request for call records would amount to an unjust invasion into the privacy of the individual.[63]

3 India's position on cross-border data flows

The treatment of cross-border data flows has been among one of the most contested aspects of the Indian data protection law. It is also an area that has undergone drastic shifts during the law's evolutionary process. In 2018, the Justice Srikrishna Committee came up with a fairly stringent set of data localization norms. They identified improving law enforcement, safeguarding against threats to disruption of critical infrastructure, building artificial intelligence systems in India, and preventing foreign surveillance as the key advantages of data flow restrictions.[64]

At that point, the draft law provided for different classes of personal data and the committee recommended that at least one serving copy of all personal data should be kept on a server located in India. Further, certain categories of critical personal data, that were to be determined by the government, were to be processed exclusively in India. The committee also suggested that any data flows would be subject to requirements like permissible transferee countries designated by the government, standard contractual clauses or intra-group schemes approved by the data protection authority, and consent from the individual.

[59] People's Union for Civil Liberties v Union of India (1997) 1 SCC 30.
[60] Rule 419A, Indian Telegraph Rules, 1951. Similar rules have also been adopted for interception of information on a computer resource under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[61] Rule 8, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[62] Rule 25(2), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[63] Tarun Krishnakumar, Law Enforcement Access to Data in India: Considering the Past, Present, and Future of Section 91 of the Code of Criminal Procedure, 1973, 15 Indian Journal of Law and Technology (2019) 67, at p. 87 to 89.
[64] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 21) p. 88-93.

Following significant pushback from a cross-section of stakeholders, the 2019 version of the bill saw a comparatively diluted version of these proposals. It did away with the data mirroring requirement for all types of personal data. It, however, maintained such a provision in respect of sensitive personal data while retaining the requirement that critical personal data would be processed only in India. Subsequently, the JPC also echoed its support for having such restrictions in the law.

As per the JPC, the motivations for localization included national security and law enforcement interests, better informational privacy, employment generation and other economic benefits, and strengthening India's bargaining powers in international interactions.[65] In addition, the JPC suggested tightening the draft provisions on conditional transfers in a few ways. For instance, they proposed that transfers based on a contract or intra-group scheme should not be approved if such an instrument goes against public policy or the state policy of India. This was defined as situations where the instrument "promotes the breach of any law or is not in consonance with any public policy or State policy in this regard or has a tendency to harm the interest of the State or its citizen".[66]

The 2022 version of the bill and the DPD Act, however, ended up doing a volte-face on the previous recommendations. The draft bill put out by MeitY in 2022 opted for what may be called a 'whitelisting' approach. It provided that the government would notify the countries to which data could be transferred and the terms and conditions for such transfer. While some saw this as a reversal of the localization mandate, the provision could also be interpreted to mean that all data transfers would be prohibited, until specified otherwise by the government. In the end, the DPD Act of 2023 chose to replace this with a more liberal 'blacklisting' approach that is described below.

3.1 Data transfers under the DPD Act

Section 16 of the DPD Act provides that the government may notify specific countries or territories the transfer of personal data to which would be restricted. This effectively means that all transfers will be permitted, unless specified otherwise. In addition to the possibility of country-specific restrictions, the DPD Act also reserves space for other laws that may impose 'a higher degree of protection for or restriction on transfer of personal data'.[67] The law does not set out any grounds or criteria that the government must take into account while notifying the restricted destinations. However, it introduces some element of accountability in such decisions by providing that the notification will have to be placed before the Parliament to enable scrutiny and allow for its modification or cancellation by the Parliament.[68]

While the Indian law does not speak of the role of contractual arrangements or model clauses in the context of data transfers, it does contain general requirements relating to arrangements with data processors. As per Section 8(2), data fiduciaries can engage data processors to process personal data on their behalf only under a valid contract. The contents of such a contract have not been outlined in the law. Neither does it mandate the government to issue any rules or guidelines in this regard. The DPD Act, however, makes it clear that the data fiduciary would continue to remain fully responsible for compliance with the law in respect of any processing undertaken on its behalf by a processor. The Act also makes specific references to ensuring compliance by processors in a few contexts, like maintaining reasonable security safeguards to prevent personal data breach, erasure of data upon

[65] Report of the Joint Parliamentary Committee (n 34), p. 41.
[66] Report of the Joint Parliamentary Committee (n 34), p. 111-112.
[67] Section 16(2), DPDP Act 2023.
[68] Section 41, DPDP Act 2023.

expiry of the retention period, and to cease processing the personal data of a data principal if they withdraw their consent.[69] Further, the data principal's right to information access includes information about the identities of all data processors with whom their data has been shared along with a description of the shared data.[70]

Therefore, even though not mandated by the law, there could be a role for the emergence of standard contractual clauses that are in line with the DPD Act to govern the relationship between data fiduciaries and processors. This could support the legal requirements of there being a valid contract between the data fiduciary and the data processor and the fiduciary remaining responsible for the activities of its processors.

Taking into account the interests of the Indian outsourcing and business processes management industry, the DPD Act also carves out an exception for such arrangements. It exempts the processing of data under a contract between a person outside India and a person based in India, as long as it does not relate to data principals in India, from a bulk of the provisions of the Act.[71] A provision of this nature could also be linked with the concept of 'data embassies' that was put out by the Indian Finance Minister in her 2023 budget speech.[72] Such data embassies could serve as corridors of trust through which governments, and possibly private actors too, would be able to locate their data in another jurisdiction without being subject to the local laws of that jurisdiction. India is yet to issue any policy directions on the mechanisms and legal framework governing this proposal.

3.2 Sector-specific restrictions

Although the DPD Act has settled on a fairly liberal position toward data transfers, India already sees a number of restrictions on data flows across sectors. Such restrictions, which are described further in the table below, can be grouped into the following four buckets: i) data pertaining to financial services, ii) data of telecommunications and broadcasting subscribers, iii) corporate and compliance data, and iv) government data.[73]

Table: Data flow restrictions in India

[69] Sections 8(5 and (7) and Section 6(6), DPDP Act 2023.

[70] Section 11(1)(b), DPDP Act 2023.

[71] Section 17(1)(d), DPDP Act 2023.

[72] Sai Ishwarbharath, Romita Majumdar and Surabhi Agarwal, Govt may notify data embassy policy as part of new Data Bill, The Economic Tines (3 February 2023) <https://economictimes.indiatimes.com/tech/technology/govt-may-notify-data-embassy-policy-as-part-of-new-data-bill/articleshow/97560396.cms>.

[73] Smriti Parsheera, What's Shaping India's Policy on Cross-Border Data Flows? in Evan A. Feigenbaum and Michael R. Nelson (eds), *How India and Korea Can Drive New Thinking About Data*, Carnegie Endowment for International Peace (2022) <https://carnegieendowment.org/2022/08/31/what-s-shaping-india-s-policy-on-cross-border-data-flows-pub-87769>.

Category	Authority	Instrument	Provision
Financial services			
Payments data	Reserve Bank of India	Directive on Storage of Payment System data, 2018	All data related to payment transactions has to be stored on a system only in India. Limited exception for cross-border payments.
Insurance policyholder records	Insurance Regulatory and Development Authority of India	Outsourcing of Activities by Indian Insurers Regulations, 2017	Insurer to ensure compliance of local laws while outsourcing services. Original policyholder records need to be maintained in India, which implies that a transfer is possible subject to this condition.
Video KYC data	Reserve Bank of India	Master Direction on Know Your Customer, 2021	Data and recordings of customer KYC to be stored on systems located in India.
Telecommunication and broadcasting			
Telecommunication subscriber data	Department of Telecommunications	Unified License Agreement	Cannot transfer user's accounting information to persons/ place outside India. Exception for international roaming
Broadcasting subscriber data	Department for Promotion of Industry and Internal Trade	Consolidated Foreign Direct Investment Policy, 2020	Cannot transfer subscribers' databases to any persons/place outside India unless permitted by law
Corporate and compliance			
Books of companies' accounts	Ministry of Corporate Affairs	Companies (Accounts) Rules, 2014	Back-up of the books of account must be kept on servers physically located in India
Risk and compliance data of financial institutions	Securities and Exchange Board of India	Advisory for Financial Sector Organizations	Institutions utilizing software as a service must keep critical data relating to risk, audits, and compliance within India.
Logs of all ICT systems	Indian Computer Emergency	Directions under Information Technology Act,	Service providers, intermediaries, data centers, body corporate and government organizations need to

	Response Team (CERT-In)	2000	keep ICT system records in India for a rolling period of 180 days.
Government data			
Public records	Parliament, National Archives of India, and the Ministry of Culture	Public Records Act, 1993	Cannot take public records out of India without prior approval of the central government, except if sent out of India for any official purpose
Cloud storage of government data	Ministry of Electronics and Information Technology	Guidelines on Contractual Terms for Cloud Services	Data center facilities and the physical and virtual hardware should be located within India
Shareable data held by the Indian government	Department of Science and Technology	National Data Sharing and Accessibility Policy, 2012	Open government data platform to be managed and hosted at the National Data Centre of the National Informatics Centre

Source: Parsheera, What's Shaping India's Policy on Cross-Border Data Flows?, Carnegie Endowment for International Peace (2022)

A few general observations emerge from the table. To begin with, there are clear variations in the types of restrictions that have been imposed across and even within related sectors. For instance, while payments-related data has to be stored only in India (subject to limited exceptions), the records of insurance policyholders can be sent abroad so long as the original record is kept in India. This may be the case because the restrictions have been introduced by a range of different actors, across ministries and statutory regulators, which may have differing priorities and approaches.

Further, the nature of instruments utilized to bring about the restrictions also varies widely. Barring the Public Records Act, 1993, which restricts the transfer of public data outside the country, all of the other restrictions emerge either from subordinate legislation like rules, regulations and directives or from other sources like telecommunication licenses, foreign investment policies, advisories and procurement contracts. Finally, as observed elsewhere, many of these requirements came about through processes that were found to be lacking in terms of transparency and deliberative policy-making.[74]

3.3 International arrangements

India has established inter-governmental channels for information sharing through partnerships with several countries. It is a member of INTERPOL, which enables sharing of police information globally

[74] Rishab Bailey and Smriti Parsheera, Data localisation in India: Paradigms and processes, CSI Transactions on ICT 9, 137–150 (2021) <https://doi.org/10.1007/s40012-021-00337-4>.

and has entered into bilateral mutual legal assistance treaties for cooperation and assistance in criminal matters, including through data exchange provisions, with 42 countries.[75] Further, mechanisms like the Quad alliance and the recent joint statement between India and the US point to arrangements for information sharing on cyber threats and vulnerabilities issues.[76] India also hosts the Information Fusion Centre – Indian Ocean Region, an alliance with 25 partners for information sharing on maritime safety issues.[77]

The EU-India Trade and Technology Council was announced in 2022 to facilitate bilateral cooperation, trade and investment between the two regions. The working group on 'strategic technologies, digital governance and digital connectivity' launched under this initiative is working towards increasing interoperability between India's and the EU's digital public infrastructure.[78] In 2022, India and the EU also signed a joint declaration on privacy and the protection of personal data along with other partners from the Indo-Pacific region, including Australia, the Republic of Korea, Singapore, and Sri Lanka.[79] The statement speaks of international cooperation on privacy and data protection. It also refers to the importance of data free flow with trust and building 'safeguards for international transfers to enable cross-border data flows by ensuring that the protection travels with the data'.[80]

As a member of G20, India has endorsed the concept of 'data free flow with trust' in ministerial declarations made by the group. The New Delhi declaration made at the 2023 G20 meeting saw a significant emphasis on the role of digital public infrastructure for advancing growth and development. In this context, the G20 members highlighted the role of 'data free flow with trust and cross-border data flows while respecting applicable legal frameworks'.[81] The members also reaffirmed the role of 'data for development', which was another priority area identified by India for its G20 presidency. This refers to initiatives aimed at boosting the production and use of data, particularly in developing countries, to accelerate and measure the progress toward sustainable development.[82]

India has, however, resisted becoming a part of the G20's Osaka Track discussions launched in 2019 to facilitate an international arrangement on cross-border flows to foster innovation and economic growth. This is based on India's position that international rule making on data flows is a trade-related matter and should be a subject of multilateral consensus at the level of the World Trade Organization

[75] Ministry of Home Affairs, Guidelines on Mutual Legal Assistance in Criminal Matters (4 December 2019) <https://www.mha.gov.in/sites/default/files/2022-08/ISII_ComprehensiveGuidelines16032020.pdf>.

[76] The White House, Joint Statement from the United States and India (22 June 2023) <https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/22/joint-statement-from-the-united-states-and-india/>.

[77] Information Fusion Centre – Indian Ocean Region <https://www.indiannavy.nic.in/ifc-ior/>.

[78] Angelos Delivorias, EU-India Trade and Technology Council - At a Glance, European Parliamentary Research Service (January 2024) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757587/EPRS_ATA(2024)757587_EN.pdf>

[79] Joint declaration on privacy and the protection of personal data (23 February 2022) <https://www.eeas.europa.eu/eeas/joint-declaration-privacy-and-protection-personal-data_en>.

[80] Ibid.

[81] G20 New Delhi Leaders' Declaration, India (9-10 September 2023) <https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf> p. 25.

[82] Thierry Soret and Hirofumi Kyunai, The G20 Contribution to the 2030 Agenda in Times of Crises 2019-2023, United Nations Development Programme and the Organisation for Economic Cooperation and Development (2023) <https://www.undp.org/sites/g/files/zskgke326/files/2023-11/undp-oecd-the-g20-contribution-to-the-2030-agenda-in-times-of-crises-2019-2023-v2.pdf> p. 61.

(WTO).[83] Further, India has also maintained that data constitutes 'a part of national wealth' and developing countries should have an equal say in furthering the use of data for trade and development.[84] For similar reasons, India is not among the 90 countries that are participating in the WTO Joint Initiative on E-commerce,[85] which is not a part of the WTO's formal multilateral negotiations process – it is an alternative plurilateral track being pursued among a subset of the WTO members.

Finally, issues of privacy and free flow of data have also come up to a limited extent in the context of India's bilateral and regional trade agreements. The India–Singapore Comprehensive Economic Cooperation Agreement identifies the importance of privacy protections but also cautions against this becoming an 'arbitrary or unjustifiable discrimination against the other Party or its investors' or a disguised restriction on investments or trade.[86] The agreement between India and Japan contains a provision on the transfer and processing of financial information. It restricts the parties from taking 'measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means' where such transfers are necessary for the conduct of the ordinary business of a financial service supplier.[87] However, it is clarified that the parties are not restricted from adopting measures to protect personal data and privacy so long as such right is not used to circumvent the provisions of the agreement.

In 2022, India entered into a comprehensive economic partnership agreement with the UAE. Following a light-touch approach, the agreement provides that the parties 'shall endeavor to promote electronic information flows across borders subject to their laws and regulatory frameworks'.[88] India is now in the process of negotiating a free trade agreement with the UK in which the latter is keen on including more definitive provisions on free cross-border flows and restrictions on data localization.[89] While the DPD Act has brought some clarity regarding India's position on these issues, it has left the door open for data flow restrictions under other laws suggesting that India may still demand to retain domestic policy space on this issue.

Its cautious approach towards data flow discussions in international agreements is also reflected in the ongoing discussions on the Indo-Pacific Economic Framework for Prosperity. Launched in 2022 as a US-led initiative, this framework seeks to foster 'cooperation, stability, prosperity, development,

---

[83] Ministry of External Affairs, "Transcript of Media Briefing by Foreign Secretary After BRICS Leaders' Informal Meeting in Osaka," Indian Ministry of External Affairs (28 June 2019) <https://www.mea.gov.in/media-briefings.htm?dtl/31516/Transcript_of_Media_Briefing_by_Foreign_Secretary_after_BRICS_Leaders_Informal_meeting_in_Osaka>.

[84] Ibid.

[85] WTO Joint Initiative on E-commerce <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm#participation>.

[86] Articles 6.11(1) and 7(1), Comprehensive Economic Cooperation Agreement between India and Singapore. Also see World Economic Forum, Advancing Data Flow Governance in the Indo-Pacific: Four Country Analyses and Dialogues (April 2021) <https://www3.weforum.org/docs/WEF_Data_Flow_Governance_2021.pdf> p. 9-10.

[87] Annex 4, Section 6, Comprehensive Economic Cooperation Agreement between India and Japan <https://commerce.gov.in/wp-content/uploads/2021/01/IJCEPA_Basic_Agreement.pdf>.

[88] Article 9.11, Comprehensive Economic Partnership Agreement (CEPA) between India and the United Arab Emirates (2022) <https://commerce.gov.in/wp-content/uploads/2022/03/Chapter-9.pdf>.

[89] Amiti Sen, India-UK FTA: Efforts on to iron out contentious areas like IPR, digital trade, environment, labour, Hindu Businessline (14 July 2023) <https://www.thehindubusinessline.com/economy/india-uk-fta-efforts-on-to-iron-out-contention-areas-like-ipr-digital-trade-environment-labour/article67080214.ece>.

and peace' among 14 countries in the Indo-Pacific region.[90] The framework is structured around four pillars – trade, supply chains, clean economy and fair economy. Of these, India has joined all the pillars except the first one on trade, which includes discussions on cross border data flows. As of now, India has chosen to maintain an observer status in the discussions under this pillar.[91] The direction of the discussions under the trade pillar, and indeed India's approach towards it, may, however, change in light of the US Trade Representative's announcement of the reversal in the US's position towards pursuing data free flow provisions in WTO discussions.[92] Similar to India's stated position on this issue, the US now seems to be interested in reserving space for domestic policy making on issues relating to data governance, privacy, competition and online regulation, prioritizing these over the free flow of data.[93]

4 Analysis and conclusion

India's evolving position on data protection has been influenced by a range of factors. When the deliberations process began in 2017, India had recently recognized the fundamental right to privacy. The GDPR came into effect around the same time and it became a logical base for the formulation of India's first draft bill, although there were some notable divergences, as with the issue of data localization. By the time the DPD Act came to be enacted in 2023, the policy mood had shifted towards a more light touch approach. This is reflected in the leaner scope and structure of the law, which now covers only digital data, has a reduced breadth of rights and obligations, and replaces the idea of a data protection regulator with a board that has a narrower enforcement mandate. This shift was accompanied by a conscious distancing from the idea of borrowing from frameworks like the GDPR and assertions of India's independent standards of data regulation.[94]

The dilution in the restrictions on cross border data flows also speaks to this move toward a leaner regulatory framework. Yet, while the DPD Act adopts a fairly liberal approach towards data transfers – of all transfers being permitted unless restricted – it leaves the field open for the emergence of other sector-specific restrictions. India already has numerous such requirements, in fields like payments, telecommunications, and for public records. It is possible that sectoral localization mandates will continue to proliferate over time.

The DPD Act does not contain any guidance to inform the rationale or processes to be followed by different agencies while adopting such restrictions or by the government while notifying restricted countries. To mitigate these concerns and prevent further fragmentation in the approach, it is

[90] Office of the United States Trade Representative, Indo-Pacific Economic Framework for Prosperity <https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef>. The participating countries are Australia, Brunei, Fiji, India, Indonesia, Japan, Republic of Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand, Vietnam and the United States of America.

[91] Ministry of Commerce and Industry, Government of India, Indo-Pacific Economic Framework for Prosperity (IPEF) Supply Chain Agreement signed by the 14 IPEF Partners, Press Information Bureau (17 November 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1977529>.

[92] David Lawder, US drops digital trade demands at WTO to allow room for stronger tech regulation, Reuters (26 October 2023) <https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/>.

[93] Patrick Leblond, After USTR's Move, Global Governance of Digital Trade Is Fraught with Unknowns, Centre for International Governance Innovation (11 December 2023) <https://www.cigionline.org/articles/after-ustrs-move-global-governance-of-digital-trade-is-fraught-with-unknowns/>

[94] Press Information Bureau, Digital Personal Data Protection Act is a world-class legislation: MoS Rajeev Chandrasekhar (13 August 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357> accessed 30 January 2024.

recommended that the basic principles, criteria, and processes governing the formulation of data flow restrictions should be identified in the law. For instance, such proposals should be developed through a consultative process, taking into account the different alternatives of conditional transfers and adopting the least intrusive approach for meeting the identified objectives.

While the DPD Act does not specify any preferred mechanisms for data transfers, it clarifies that the appointment of a data processor has to be done pursuant to a valid contract. Accordingly, there seems to be a role for the emergence of model contractual clauses that would govern the relationship between data fiduciaries and processors in line with the requirements of the DPD Act. In the absence of any regulatory mandate for the government or the Board to frame or approve such contracts, stakeholders from the industry can voluntarily take up the initiative of developing model/ standard clauses following an open and consultative process. This can serve as a mechanism for building trust among data fiduciaries and processors and facilitating the ease of regulatory compliance.

Finally, it is important to consider how the exemptions available to state agencies for surveillance, law enforcement and other designated purposes might interact with the discussions on data flows. The DPD Act does little in terms of reforming the process for interception of communications and data access by law enforcement agencies. These aspects continue to be governed under other laws like the Information Technology Act, 2000 and the Telecommunications Act 2023, which do not have safeguards like judicial approval of information request, notice to the individual, transparency requirements, and redress mechanisms.[95] India also does not have other standalone laws to govern its surveillance and intelligence agencies. In 2011, an attempt towards bringing about such a regulatory framework was made through a private member bill drafted by a Parliamentarian, Manish Tewari.[96] The bill lapsed in 2012 and was reintroduced in the Parliament in 2019 as the Intelligence Services (Powers and Regulation) Bill, 2019 but has not seen any action since then.[97]

Further, the exceptions created under the DPD Act, particularly under Section 17(2), allow for the complete exclusion of agencies from the scope of the data protection law on grounds like sovereignty and integrity of India, security of the State, and public order. The provision also goes on to exclude any further processing by the government of the data that is furnished to it by an exempted agency. This provision may at some point be subjected to a constitutional challenge to test its validity against the fundamental right to privacy, as is already being done in a bunch of pending petitions challenging the country's existing surveillance regime before the Supreme Court.[98]

Besides being violative of citizens' privacy rights, unchecked powers of law enforcement and intelligence agencies are also detrimental to the free flows of data into the country. For instance, soon after the enactment of the DPD Act, a question came up in the European Parliament about the "interference of Indian intelligence services through digital surveillance and the Indian Parliament's

[95] Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, Use of Personal Data by Intelligence and Law Enforcement Agencies, National Institute of Public Finance and Policy (1 August 2018) <https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data>.

[96] Manish Tewari, Intelligence Agencies Need Greater Scrutiny, Congress Sandesh (12 July 2021) <https://inc.in/congress-sandesh/comment/intelligence-agencies-need-greater-scrutiny>.

[97] Intelligence Services (Powers and Regulation) Bill, 2019 <https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/249%20of%202019%20as.pdf?source=legislation>

[98] The Wire, Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State (14 January 2019) <https://thewire.in/law/supreme-court-pil-centre-snooping>.

apparent lack of control over the intelligence services' actions" and its impact on GDPR adequacy.[99] The response indicated that the European Commission was not engaged in any adequacy talks with India at that point.[100]

As shown by the Schrems II decision, the domestic surveillance and government data access regime is also relevant for other transfer mechanisms besides adequacy. Independently, the situation described above may also interfere with India's plans of boosting its data center infrastructure and inviting the setting up of data embassies – currently, there is no clarity on how the scope of surveillance powers might interact with the potential creation of such embassies. All of these factors point to the necessity of bringing legislative reforms to strengthen the surveillance and law enforcement framework in India.

To summarize, the paper makes three recommendations on issues related to cross border data flow. First, it recommends that, in order to minimize fragmentation and uncertainty, the law should set out the basic principles, criteria, and processes to govern the adoption of any sectoral data flow restrictions. The government's power to impose restrictions on data flows to specific countries should also be bound by such reasonable and identified criteria.

Second, it suggests that stakeholders from the industry can voluntarily take up the initiative of developing model/ standard clauses that would meet the requirements of the DPD Act, and ideally go beyond that, through an open and consultative process. This can serve as a mechanism for building trust among data fiduciaries and processors and facilitating the ease of regulatory compliance.

Third, the paper makes a case for legislative reforms to strengthen the country's surveillance and law enforcement framework. Besides being violative of citizens' privacy rights, unchecked powers of law enforcement and intelligence agencies are also detrimental to the flow of data into the country.

Acknowledgements:

This research has been funded by Cerre, Brussels, Belgium. The author is grateful to Sophie Stalla-Bourdillon, Pablo Rodrigo Trigo Kramcsak and Yueming Zhang for valuable inputs and discussions.

[99] Markéta Gregorová, Adequacy of India's data privacy law with regard to EU GDPR standards, Parliamentary question - P-002961/2023 (6 October 2023) <https://www.europarl.europa.eu/doceo/document/P-9-2023-002961_EN.html>.

[100] Answer given by Mr Reynders on behalf of the European Commission, Parliamentary question - P-002961/2023(ASW) (6 December 2023) <https://www.europarl.europa.eu/doceo/document/P-9-2023-002961-ASW_EN.html>.