DATA COLONIALISM AND DOCTRINAL GAPS: RETHINKING INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AI DISCLOSURE STATEMENT

The author used an AI-assisted tool for language editing, grammar refinement and citation formatting. All legal research, doctrinal analysis, arguments, and conclusions presented in the body of this manuscript (Parts I through IV) are the author's own original work, developed through iterative dictation and fact-verification.

ABSTRACT

This article examines India's Digital Personal Data Protection Act, 2023 through two lenses — the domestic approach and the global approach. Adopting a doctrinal and comparative method, it situates India's data protection regime within the broader context of global data flows, drawing on infrastructure and trade data to show how developed economies, particularly the United States, hold disproportionate control over data originating in developing countries such as India. This asymmetry, examined through the lens of data colonialism, is argued to raise concerns of economic value extraction and legal sovereignty that a purely privacy-focused reading of the DPDP Act overlooks. The article then turns inward, tracing the Act's legislative history from the Puttaswamy judgment through to its 2023 enactment, and identifies specific doctrinal gaps that limit its protective force: the absence of a sensitivity-based data category, an executive-appointed and currently non-functional Data Protection Board, an overbroad state-security exemption under Section 17, and a permissive and largely dormant cross-border transfer regime under Section 16 — illustrated through the practical difficulties these gaps create for citizens seeking redress in the Parth Sharma litigation. It concludes that meaningful reform requires judicial involvement in institutional design, a functioning cross-border enforcement framework, and greater legal sensitivity toward individual data subjects.

Keywords: Digital Personal Data Protection Act, 2023; data colonialism; data localisation; Data Protection Board of India; cross-border data transfer; right to privacy

I. INTRODUCTION

Data protection laws have emerged to safeguard individuals' privacy and digital life through different legislation and judgments. We have seen how data privacy has become a core function and aim of government bodies and the state. Whether in the European Union, the United States, or India, everyone has taken steps to protect individuals' personal data and privacy. Maintaining checks and balances on big corporations that extract personal data is the aim of all these legislations. We will look at how we can further improve these regulations, democratise them, and prioritise the concerns of individuals.

II. DATA AS THE NEW COLONIAL FRONTIER

The United States of America runs 2,600+ data centre facilities across its land, which accounts for roughly 33% of the total data centres across the globe.[1] Other countries are far from the US when it comes to data centres. The UK, which comes 2nd on the list, accounts for only 6 percent of the total data centres. Apart from data infrastructure, the USA also holds the headquarters of the corporations that own and operate these centres. This gives the USA access to personal data of individuals who may be far beyond its reach and jurisdiction. The USA uses this data to carry on its objectives, including targeting terror outfits. In October 2012, the NSA killed Hassan Ghul, who was at the time located in the remote tribal belt of Pakistan.[2] There was significant use of metadata — data that is accompanied by the digital data, including IP address, exact location of communication, devices used, and time duration of calls. In multiple instances, this has been used in West Asia and beyond. Such leverage gives the USA the power to effectively neutralize its enemies far from its shores. In addition, the USA earns big from such data. In the year 2012, US digital exports were almost $223 billion while digital imports were $106 billion, giving it a surplus of $117 billion.[3] This makes the digital economy one of the few areas where the USA

[1]U.S. Int'l Trade Comm'n, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions* 45 (2017) (copy on file with author).

[2]Greg Miller, Julie Tate & Barton Gellman, *Documents Reveal NSA's Extensive Involvement in Targeted Killing Program*, Wash. Post (Oct. 16, 2013), https://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html (last visited Aug. 22, 2026) (copy on file with author).

[3]U.S. Int'l Trade Comm'n, *supra* note 1, at 12.

does not have a severe deficit but a gigantic profit. With the USA holding such leverage, big tech companies will continue to see the USA as a haven for investment and the right place for the future multi-billion-dollar digital economy.

After the USA, Germany and China each run about 5 per cent of all data facilities, with India accounting for roughly 2 per cent.[4] The USA has more facilities than the next 10 countries on the list combined.[5] Most raw data originates in the developing world and flows through trans-Pacific and trans-Atlantic data streams to reach the USA. In the US, these centres collect, process, and store this data on cloud and platform servers. Europe, the largest developed market, provides large amounts of high-quality data to the US, while South-East Asia, with its high broadband penetration, has also driven this trans-Pacific data flow. The only exception to such enormous data migration is China, which, through its state firewall and strict data sovereignty and localisation laws, has localised its data storage.

Because of India's vast digital population, our data is also stored in the US. Data stored abroad falls outside Indian courts' jurisdiction. This may seem like a protective shield the government cannot cross to violate an individual's privacy, but big tech sells that very privacy without any laws governing it. The Indian administration is the de facto bona fide protector of its citizens' rights. Indian jurisdiction over such data would, most of the time, be a better choice than US jurisdiction.

In earlier decades, there has been news of oil spills that caused disaster for the local ecosystem. One of them was the Deepwater Horizon spill in 2010, in the Gulf of Mexico, the largest accidental marine spill.[6] Coastal and marine life had a near-death experience with this spill. In the current day and age, these spills have taken a new form — data spills, which have emerged as another man-made disaster. The latest of such was the Aadhaar data breach of 2018, which resulted in the personal details of approximately 1.1 billion people being openly available on specific websites.[7] While governments are focused on taking control of their citizens' data, they

[4]U.S. Int'l Trade Comm'n, *supra* note 1, at 45.

[5]Mappr, *Ranked: The Countries With the Most Data centres* (2025), https://www.mappr.co/countries-with-most-data-centres/ (last visited Aug. 22, 2026) (copy on file with author).

[6]Nat'l Comm'n on the BP Deepwater Horizon Oil Spill & Offshore Drilling, *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling* 1 (2011) (copy on file with author).

[7]Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-detail

should equally focus on protecting it through firewalls and identity and access management. Governments should focus on building resilient cybersecurity infrastructure, which almost every country is lagging in. This will result in continued data breaches soon.

The Mutual Legal Assistance Treaty (MLAT), which was made for digital enforcement of one single record at a time, has now proved to be the most inefficient treaty in the digital world, where data flows every second. Due to a complicated legal process and no real-time digital enforcement, there is continued breach of cross-border digital personal data. In this regard, the world needs a better and more active treaty that can treat citizens of each country as global citizens and protect their rights from big corporations. A first step in this regard can be a fast-track mutual recognition framework for data requests, where data requests are approved in real-time, resulting in enforcement equal to the speed of data flow.

Data has been termed the new oil of the 21st century.[8] Like any other resource, with the discovery of such a resource, countries try to take control of it. This is what has happened as different legislation has come into effect in different countries. But as mentioned earlier, there is a bias in such data flow, with the USA and western countries taking a lead not just in taking control of their own personal data but also that of the developing world, including India. Such bias is what many call data colonialism, a new-age colonialism where, instead of human and natural resources, first-world countries are using the data of the global south for their benefit. This term was coined by Nick Couldry and Ulises Mejias in their book.[9]

While data may seem to be just numbers and words, when in large quantities, it proves to be of great use. When raw data arrives at these centres, it gets stored in data lakes (Google Cloud Storage and Amazon S3). To clean and transform such random data, which does not have much pattern, distributed processing engines like Apache Spark, Databricks, or Snowflake are used. Here, data is converted into structured format via columns and tables. This is the process of

---

s-523361/ (last visited Aug. 22, 2026) (copy on file with author); *but see* UIDAI Press Release, *No Aadhaar Data Breach, Says UIDAI* (Jan. 2018) (copy on file with author) (denying any breach of the central database).

[8]This phrase is commonly attributed to Clive Humby, *The Data Is the New Oil*, ANA Sr. Marketers Summit (2006); *see also* Bernard Marr, *Here's Why Data Is Not the New Oil*, Forbes (Mar. 5, 2018), https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/ (last visited Aug. 22, 2026) (copy on file with author).

[9]Nick Couldry & Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019)a .

converting crude oil into refined oil for the 21st century. This data is used to train AI and feed machine learning models. One such use is a large-scale predictive model, which recommends future algorithms based on current consumption and interactions of individuals. This also helps in building end-user applications that are highly personalised based on data patterns. Another example would be business decisions taken after considering the taste and consumption trends of a market. Additionally, it helps servers automate bots and fraud alerts based on past patterns.

Till now, we have understood that the use of such data in large language models and machine learning helps markets decide on many things, make predictions, and take decisions that would change the course of our economy and business. On a personal level, when personal data is used by corporations that extract and profit from this data, that profit arguably belongs with the individuals whose data generated it. As individuals are the owners of this data at an individual level, using this data for corporate profit, at the individual's risk, amounts to a violation of privacy. That is the reason many countries are now thinking seriously about how to protect individuals' data. Startups and small domestic businesses can use such data to understand their market, rather than multinational organisations that have the resources to extract such data from developing countries. Governments around the world are bringing in legislation that localises data storage and data processing — the DPDP Act being one example, alongside laws like Russia's data localisation mandate under Federal Law No. 242-FZ[10] and China's Cybersecurity Law.

III. DOCTRINAL ANALYSIS OF INDIA'S DPDP ACT, 2023

The DPDP Act had a long way to go till it came to be known as what it is today. It all started with the Justice K.S. Puttaswamy judgment, where a nine-judge constitutional bench unanimously decided that the right to privacy is to be included under the purview of Article 21.[11] It further directed the government to legislate laws and policies for a robust statutory data protection framework. In the coming years, the government brought different alterations of the data protection bill, including the Personal Data Protection Bill, 2019, but faced backlash from

[10]Federal'nyy Zakon RF o Personal'nykh Dannykh [Federal Law on Personal Data] No. 242-FZ, 2014 (Russ.).

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

entrepreneurs and civil societies. Finally, in 2023, the DPDP Act was passed and received Presidential Assent on August 11, 2023.[12]

Alongside its legislative history, the DPDP Act has also received various criticisms. One of the most talked-about criticisms is the absence of a category that divides data into different heads based on their sensitivity. This form of division is based on the US's sectoral model of data collection. The government failed to categorise and divide different sorts of data just like how it is done in the US, where data is divided based on sector — such as health data under HIPAA, financial data under the Gramm-Leach-Bliley Act, and children's data under COPPA.[13] But the government, through the DPDP Act, completely misses out on this area. This results in the non-prioritisation of data that is really sensitive, including data related to the privacy of women, children, and marginalised communities. The Act treats all data the same and does not differentiate between them, so it loses track of which data should be prioritised first in case of a breach.

Another blind spot is the topic of the right to be forgotten, which was first put forth in Article 17 of the GDPR of the European Union, which talks about how the individual has the right to be forgotten online.[14] Going one step forward, the Italian government brought in legislation that brought cancer patients into the purview of the right to be forgotten, providing cancer survivors fair rights to banking services.[15] While taking loans, cancer survivors can use this right to erase their medical history and to easily receive loans and other banking services.

An important and core part of the DPDP Act is the Data Protection Board of India (DPBI).[16] This body aims to govern the personal data that would otherwise be unprotected. Its goal is to be an impartial dispute resolution body, but it faces significant questions. Analysts have argued that it is not independent. The chairperson and members of this body are fully and exclusively appointed by the central government, which makes it an extension of the central government

[12]Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

[13]*See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191; Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (1999); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506.

[14]Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 (*General Data Protection Regulation*), art. 17, 2016 O.J. (L 119) 1.

[15]Legge 7 dicembre 2023, n. 193 (It.) (right to be forgotten for cancer survivors) (copy on file with author).

[16]Digital Personal Data Protection Act, 2023, § 18.

itself.[17] Another thing to add is that the members hold a tenure of only two years, which makes it hard for them to make decisions while they are eligible for reappointment, but this makes the continuity and effort for justice short of time.[18] SFLC (Software Freedom Law Centre) called it "a watchdog without teeth."[19] Currently, the board does not have a single member who is actually appointed. It only exists on paper and is not functional at all. So when citizens try to seek real remedies because of violations, since this board is non-existent and non-operational, those remedies cannot be availed by the citizens. Improvements that can be made to the Data Protection Board of India include the inclusion of the judiciary in the process of appointment, by making sure that the appointments are fair and not arbitrary. The judiciary must be included, and special judicial officers should be made part of such a committee. And with such inclusion and later appointments, the body should start its functions at the quickest.

Section 17 of the DPDP Act talks about the exceptions to such data use and collection.[20] It talks about how, for research purposes, individual data can be used by institutions. This can be a big loophole to bypass consent, where organisations can simply tag data as being for research purposes and use it without getting any consent from the individuals involved in the data. Contrarily, the government is also given a free hand by using the specific terms "sovereignty and integrity of India" or "maintenance of public order" in the definition itself.[21] This results in a very vague exception that can be used broadly by the government to bend its ways to use personal data for its benefit, violating the privacy of fellow citizens.

Section 16 of the DPDP Act talks about cross-border data transfer.[22] This provision talks about the blacklisting process and how the government can blacklist certain countries from receiving data of Indian citizens. It is the opposite of the model used by the European Union's GDPR.[23] The GDPR releases a list of approved countries through which only the data can flow, while India follows a negative list. This gives certain institutions leverage by going through third-party

[17]Digital Personal Data Protection Rules, 2025, r. 17.

[18]Digital Personal Data Protection Act, 2023, § 20.

[19]Software Freedom Law Centre, India, *Comments on the Data Protection Board* (copy on file with author).

[20]Digital Personal Data Protection Act, 2023, § 17(2)(b).

[21]Digital Personal Data Protection Act, 2023, § 17(2)(a).

[22]Digital Personal Data Protection Act, 2023, § 16.

[23]Regulation 2016/679, *supra* note 14, arts. 44-46.

countries, taking advantage of and using the data of Indian citizens while remaining fully legal and free to use it, as they are not in a blacklisted country. In addition, it is also an arbitrary process, as it is only the executive that can decide which country should be blacklisted and which should not. Based on the benefits the government receives, it can trade off individuals' personal data for leverage or for profits that are unseen or cannot be tracked publicly. Furthermore, currently no such list exists that restricts such data transfer, which means any country in the whole world can, through data transfers, access Indian citizens' personal data.[24]

In the case of Parth Sharma v. Union of India, before the Madhya Pradesh High Court, the petitioner had approached the court for remedies regarding Instagram's proposed discontinuation of end-to-end encrypted messaging, framed as a violation of the right to privacy.[25] In defence, the government said that the petitioner had not exhausted the remedy provided under the DPDP Act — that is, the DPBI — which one must approach before the matter can be escalated further, including eventually to TDSAT (the Telecom Disputes Settlement and Appellate Tribunal) on appeal. But the fact of the matter was that the Board was not operational yet. The government had not appointed a single member to the Board, which meant the petitioner could not actually seek remedy, as the Board itself did not exist to be approached. Regarding TDSAT, it is a body that was originally set up for disputes relating to telecom regulation and its implementation, but it is now expected to handle, through the DPDP Act, cases related to data privacy breaches, which it does not specialise in.

IV. CONCLUSION

To conclude, the DPDP Act needs real improvements, including the adoption of a right to be forgotten. It needs a more robust process for grievances against violations of individual privacy, and it needs greater sensitivity towards individuals alongside a more hardline approach towards

[24]As of mid-2026, the Central Government has not issued any notification identifying restricted countries under Section 16; *see* Mondaq, *Cross-Border Data Transfers Under India's DPDP Framework: Navigating The New Compliance Landscape* (2026), https://www.mondaq.com/india/privacy-protection/1828534/cross-border-data-transfers-under-indias-dpdp-framework-navigating-the-new-compliance-landscape (last visited Aug. 22, 2026) (copy on file with author).

[25]*Parth Sharma v. Union of India*, Writ Petition (PIL) (M.P. High Court, Indore Bench, order dated Apr. 9, 2026), as reported in *Madhya Pradesh High Court Sends Instagram Encryption Challenge to Data Protection Board*, LawBeat (Apr. 13, 2026), https://lawbeat.in/news-updates/madhya-pradesh-high-court-sends-instagram-encryption-challenge-to-data-protection-board-1580618 (copy on file with author).

big corporations. Meaningful reform would mean introducing a sensitivity-based category for personal data, bringing the judiciary into the process of appointing members to the Data Protection Board, adopting a faster and more active cross-border enforcement framework in place of the current MLAT system, and ensuring that the cross-border transfer blacklist under Section 16 is actually activated and maintained rather than left dormant. Taken together, these changes would move the DPDP Act closer to the robust statutory framework that the Puttaswamy judgment originally called for.