CROSS-BORDER DATA FLOWS AND THE QUESTION OF DIGITAL SOVEREIGNTY: A LEGAL ANALYSIS

Abha Katiyar, ABVSLS, Chhatrapati Sahu Ji Maharaj University Theme: Data Protection, Privacy and Digital Sovereignty

Dr. Divyansh Shukla, Research Scholar, ABVSLS, Chhatrapati Sahu Ji Maharaj University Theme: Data Protection, Privacy and Digital Sovereignty

ABSTRACT

In the faster than ever developing economy and world, which is skyrocketing towards the digital world. The cloud market in India is expected to reach a projected revenue of US$ 76,385.7 million by 2030[1] and India is the world's 3rd-largest digitalized economy[2]. Data privacy is one of the foundational pillars, for digital sovereignty, the corollary being that the states autonomy and ability to protect their digital infrastructure or data, independent of any influences and foreign actors. In conjunction with the above, the free data flows that is essential for the global digital economy, thereby putting in motion the cross-border transfer of the data, that enumerates the fundamental aspect of global trade, which immediately creates a center of tension between the idea of digital sovereignty and cross-border flow of the data.

The state's paramount obligation to safeguard the privacy of the citizens and its individuals, must be balanced against the potential consequences of restricting cross-border data flows, imposing strict data localization, which eventually could undermine the global economic and trade interests, thus necessitating a nuanced legislative framework that protects the individual's privacy while facilitating secure and regulated data exchange to foster economic growth. The major research question is to examine what legislative and regulatory measures a state implements to manage privacy and personal data of their individuals, that is prone to cyber-crime and synchronically restrictions on the cross-border data flow, do not depreciate the quality of international trade and economic growth of the nation, in accordance with national and international framework. This research is based on mixed-method approach of doctrinal and non-doctrinal research techniques, in the

[1] *India Cloud Computing Market Size & Outlook, 2030*. (2026, March 9). https://www.grandviewresearch.com/horizon/outlook/cloud-computing market/india#:~:text=The%20cloud%20computing%20market%20in,market%20from%202025%20to%202 30.&text=U.S.

[2]Government of India. (2026, January 27). *Strengthening confidence in India's evolving digital ecosystem* [Press release]. Retrieved March 19, 2026, from https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2219070®=3&lang=2#:~:text=Notified%20on%2013 %20November%202025,and%20unauthorised%20exploitation%20of%20data.

paper which essentially involves the collection quantitative and legal approach and then the analysis of the collected data from the different scholars and authors. As cyber-crime and digital sovereignty is a complex research topic, this method provides comprehensive and descriptive analysis of the GDPR, DPDP Act, 2023 and various other regulations.

Keywords: Digital sovereignty, cross-border data flow, data localization, digital governance, cybersecurity.

CHAPTER 1

INTRODUCTION

"Data is a precious thing and will last longer than the systems themselves."

- Sir Timothy John Berners-Lee

1.1 INTRODUCTION

In a data driven world, where data is a 'present-day gold', with a population of exceeding 1.4 billion, and over 900 million internet users, and a rapidly growing digital services market, leading India towards being world's 3rd-largest digitalized economy[3], thereby imposing an obligation on the state to ensure protection of the personal data to safeguard the privacy of the individuals. The supreme court of India has progressively recognized privacy as a fundamental right, in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[4]. The personal data of the individuals which are very much prone to cyber-crime and these crimes are moving forward in large-scale breaches of personal data posing several challenges and concerns to the nation as well. Furthermore , the concept of 'colonialism' has not yet disappeared from the world; it has just taken a new form, our data.[5] 'Data colonialism' wherein the foreign tech corporations extract data from the individuals of nations in order to fuel the artificial intelligence and enlarge their economic growth, which has led to the emergence of the concept of the digital sovereignty, and additionally the rise

[3] Government of India. (2026, January 27). *Strengthening confidence in India's evolving digital ecosystem* [Press release]. Retrieved March 19, 2026, from https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2219070®=3&lang=2#:~:text=Notified%20on%2013%20 November%202025,and%20unauthorised%20exploitation%20of%20data.

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

[5] *What is data colonialism?* (n.d.). The London School of Economics and Political Science. https://www.lse.ac.uk/lse-player/what-is-data-colonialism

of the Internet, has interconnected the world in ways that have transcended traditional borders, creating opportunities for economic growth, cultural exchange, and innovation by cross-border data transferring. However, these advancements have also introduced a new landscape of risks, including data security threats, cyberattacks, and the weaponization of information.[6]

1.2 CONCEPT OF DIGITAL SOVEREIGNTY AND CROSS-BORDER DATA TRANSFER

Digital sovereignty describes the ability and autonomy of a state to protect their own jurisdictional digital infrastructure or personal data of their individuals, independent of any of the influences and foreign actors. In simple words, Digital sovereignty, cyber sovereignty, technological sovereignty, and data sovereignty refer to the ability to have control over your own digital destiny the data, hardware, and software that you rely on and create.[7](World Economic Forum 2025.)

Meanwhile cross-border data transfer, is defined as ability to transfer data internationally.[8] The phrase "cross-border data flows" refers to the movement or transfer of digital information between servers located in different countries.[9] The simple meaning, can be concluded as the sharing of the personal data of the individuals across the international borders, it may involve legal and regulatory complexities due to regional data protection and privacy variations.[10] In today's digital economy the data is used at a daily basis by the companies, corporations, by HRs at global level at an international level, thereby letting the data flow across internationally so as to regulate the international trade and boost the economy. As also noted by the Organization for Economic Co-operation and development (OECD), "the ubiquitous exchange of data across borders has amplified a range of concerns for governments, businesses and citizens, eroding trust among them."[11] This certainly helps

[6] Hwang, J. Y. (2025). Digital sovereignty in an era of cyber threats and global connectivity. *International Journal of Multidisciplinary Research Updates*, *9*(2), 012–023. https://doi.org/10.53430/ijmru.2025.9.2.0023

[7] *What is digital sovereignty and how are countries approaching it?* (2026, January 5). World Economic Forum. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

[8] Nguyen, D., Paczos, M., & UK Economic Statistics Centre of Excellence. (2020). Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective. *OECD DIGITAL ECONOMY PAPERS*, No. 297.

[9] *Cross-border data flows and free trade agreements*. (2024, November 1). Digital Trade Alliance. https://dtalliance.org/2024/01/05/cross-border-data-flows-and-free-trade-agreements/

[10] Securiti. (n.d.). *Cross-border data transfer*. https://securiti.ai/glossary/cross-border-data-transfer/

[11] Francesca Casalini et al., *Cross-border data flows: Taking stock of key policies and initiatives*, OECD, October 2022, https://read.oecd-ilibrary.org/science-and-technology/cross-border-data-flows_5031dd97-en#page4

and promotes the international trading and economy of the states, but it possesses certain threat over the national security of the state and to the privacy of the individuals, by interfering in their personal data autonomously.

1.3 STATEMENT OF PROBLEM

The rapid growth of technology and digitization, worldwide which has led to a surge in cross-border data flows, corollary being that the data of a certain jurisdiction, is shared to the other jurisdictions, which eventually facilitates the international trade, innovation, and communication among the nations worldwide. This unblemished flow of data, cross boundaries, has raised critical privacy related concerns, national security and the regulatory frameworks among the jurisdictions.

1.4 AIMS AND OBJECTIVES OF STUDY

Aims-

1. The present study extends to gather extensive data on the cases of

2. The study would further examine the role played by the legislative, and the judiciary in combating and balancing the issue of privacy of the personal data and protection of the nation from cyber-crime, by implementing restrictions on the free flow of the data, but without depreciating the international trade and economy.

3. The study would also determine the defects in the available laws and proximate causes of failure to address digital sovereignty in the nation.

4. The study would also examine the international and national framework in elevating and implementing digital privacy as a foundational pillar of data protection.

Objectives-

1. To examine and define the concept of digital sovereignty and the free flow of data in the digital landscape.

2. To examine all the international and national frameworks and the principles governing cross-border data transfers.

3. To analyze and compare the different regulatory approaches adopted by the major jurisdictions recently, such as the European Union, the United States, China and India.

4. To study the Indian legal framework relating to data protection, privacy, and data localization.

5. To identify the key legal and policy challenges arising from the conflict between data flows and digital sovereignty.

6. To evaluate the impact of data regulation on trade, innovation, and individual rights.

7. To suggest reforms and recommend a balanced legal framework that harmonizes global data flows with sovereign interests.

1.5 RESEARCH METHODOLOGY

This study adopts a doctrinal, comparative and empirical research methodology, formulated to the multi-dimensional nature of the research problem. The primary methodological approach involves a systematic analysis of primary legal sources, including statutes, regulations, circulars, judicial decisions, and quasi-judicial orders, which are the secondary sources. Thereafter, there is comparative legal research wherein a structured analysis will be undertaken from the European Union, UN model of free flow of data, China's model of data sovereignty and free flow of data across the borders.

Cross- Border Data Flow

The phrase "cross-border data flows" refers to the movement or transfer of digital information between servers located in different countries.[12] The simple meaning, can be concluded as the sharing of the personal data of the individuals across the international borders, it may involve legal and regulatory complexities due to regional data protection and privacy variations.[13] In today's digital economy the data is used at a daily basis by the companies, corporations, by HRs at global level at an international level, thereby letting the data flow across internationally so as to regulate the international trade and boost the economy. As also noted by the

[12] *Cross-border data flows and free trade agreements*. (2024, November 1). Digital Trade Alliance. https://dtalliance.org/2024/01/05/cross-border-data-flows-and-free-trade-agreements/
[13] Securiti. (n.d.). *Cross-border data transfer*. https://securiti.ai/glossary/cross-border-data-transfer/

Organization for Economic Co-operation and development (OECD), "the ubiquitous exchange of data across borders has amplified a range of concerns for governments, businesses and citizens, eroding trust among them."[14] This certainly helps and promotes the international trading and economy of the states, but it possesses certain threat over the national security of the state and to the privacy of the individuals, by interfering in their personal data autonomously.

This flow of data is done in many ways-

1. Engaging third party vendors, or third-party service providers in order to supply data, to store, access or to process data from certain applications to facilitate a third-party app as well, which in turn uses the personal data and have all the access to the data of the individuals, internationally.

2. Necessitating the cookie features for performing actions of enrichment (Winks, 2025) [15] and doing analysis of the data of the individuals.

3. International payments and financial assistance, there are many businesses functioning internationally and they have been performing their functions across the boundaries, thereby mandating the financial work across the borders.

4. Engaging and hosting data on cloud servers, that makes information and data accessible and are operated by the third parties, for pooling the data. (Susnjara & Smalley, n.d.)[16]

Cross-border data transfers role in shaping the digital economy

In a digital economy, cross-border data flows are crucial in enabling improvements in national economies and living standards in developing countries. (United Nations Capital Development Fund, 2022) [17] The seamless transfer of data across the borders supports global trade, innovation and communication. As, in the present digital world, the businesses are heavily relying on the digital infrastructure, thereby mandating them to depend heavily on the personal

[14] Francesca Casalini et al., *Cross-border data flows: Taking stock of key policies and initiatives*, OECD, October 2022, https://read.oecd-ilibrary.org/science-and-technology/cross-border-data-flows_5031dd97-en#page4
[15] Winks, E. (2025, June 24). *Cross-border data transfers: How to stay compliant globally in 2025*. Atlan. https://atlan.com/know/data-governance/cross-border-data-transfers/
[16] Susnjara, S., & Smalley, I. (n.d.). *What is cloud hosting?* IBM. https://www.ibm.com/think/topics/cloud-hosting
[17] United Nations Capital Development Fund. (2022, July 22). *The role of cross-border data flows in the digital economy*. UNCDF Policy Accelerator. https://policyaccelerator.uncdf.org/all/brief-cross-border-data-flows

data of the individuals for the smooth conduct of their businesses.

The most significant role played by the flow of data across the boundaries is by facilitating international trade with digital services and data. The flow of the

CROSS-BORDER DATA FLOWs as a Legal Concept

The expression Cross-Border Data Flows looks simply, but legally it is much wider than the movement of a file from one country to another.[18] In a normal understanding, the cross-border flow of data is understood as mere physical transfer of the data from one country to another country, but an exhaustive set of activities involving the data across the jurisdictions, including: transfer, storage, access, processing, and disclosure to third parties and foreign entities all of these constitute the cross-border data flow, and a legally nuanced understanding acknowledges that even if data is not physically transferred across the borders, but is anyhow made accessible to the other jurisdiction, there they constitute the cross-border data flow. There is no unified law for the regulation of cross-border data flows therefore the defining factor is not constructed yet, because the legal frameworks for this are very fragmented and are absent from a single page.

This expansive interpretation is broadly reflected in the General Data Protection Regulation (GDPR) under Article 4(1), which defines 'personal data' broadly as any information relating to an identified or identifiable natural person[19], thereby creating a wide spectrum for the regulation of the data shared across the borders to other jurisdiction.

Furthermore, Chapter V of GDPR 'transfer of personal data to third countries or international organizations'[20] wherein Article 44 mentions the general principles for transfers[21] of data across the jurisdictions, and Article 46[22] simultaneously describes, transfer would be subjected to appropriate safeguards, which provides adequate safeguards, such as adequacy decisions, standard contractual clause, or binding corporate rules. These provisions specifically govern

[18] Santos, E. A. (n.d.). *Cross-border data flows in international law*. Diplomacy & Law. https://www.diplomacyandlaw.com/post/cross-border-data-flows-in-international-law
[19] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 4(1)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[20] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Chapter V*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[21] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 44*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[22] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 46*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

the restricted cross-border data flow, which are the compliance requirements so as to protect the data of the individuals.

Thus, cross-border data flows represent a dynamic and multifaceted legal concept situated at the intersection of technology, law, and global governance. The regulatory approaches adopted under instruments like the GDPR and India's Digital Personal Data Protection Act, 2023 highlight the evolving effort to balance the free flow of data with the imperatives of privacy, security, and digital sovereignty, making this concept central to contemporary debates in international data governance.

Understanding 'DIGITAL SOVEREIGNTY': Origin and evolution

In the recent politics of Europe[23], the word 'digital sovereignty' is widely dealt with. It's important to understand the term, Digital sovereignty, cyber sovereignty, technological sovereignty and data sovereignty refer to the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create.[24] Digital sovereignty and digital governance are two corresponding concepts, as sovereignty cannot be achieved without proper governance. The idea of sovereignty is elaborated as autonomy over the data collected within the national borders, independent of the outside influence and actors and is sovereign. Quite simply, (C. Mathew Snipp)[25] explains data sovereignty as managing information in a way that is consistent with the laws, practices and customs of the nation-state in which it is located. It is sometimes referred as strategic autonomy, or technological sovereignty that has emerged as the discursive tool to enable institutions to determine their strategic interests, and promote them, and even project them on the rest of the world.

In this dynamic environment, a focus on the notions of trust and accountability emerges, as areas where the dynamic driving public administration and digital sovereignty coincide. As the multilateral world order, that has been defining feature of the international system since world war-II has been challenged by the democratic backsliding in young and old democracies alike, and most notably in the sense of a decline in the trust of politicians and political parties, states

[23] European Commission. (n.d.). *Data protection*. Retrieved April 12, 2026, from https://commission.europa.eu/law/law-topic/data-protection_en

[24] Fleming, S. (2025, January 10). *What is digital sovereignty and how are countries approaching it?* World Economic Forum. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

[25] Mishra, N., & Mitchell, A. D. (2021). *WTO law and cross-border data flows: An unfinished agenda*. In M. Burri (Ed.), *Big data and global trade law* (pp. 83–112). Cambridge University Press. https://doi.org/10.1017/9781108919234.006

are starting to change the way they present themselves on both international and domestic scenes. They are starting to claim over transnational actors, attempting to 'take back control' over the domestic markets. In the digital sphere, this has become a highly poignant issue, with core debates around the power of the multinational corporations that are often portrayed as being 'beyond the reach' of policymakers. Critical infrastructure management, or protection of critical infrastructure is one way in which the governments are making increased moves to ensure that they have control, or sovereignty, over their territory.[26]

EUROPEAN UNION GDPR as the Global Privacy Benchmark

The right to privacy is part of the 1950[27] European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence."[28] From this basis, the European Union has sought to ensure the protection of this right through legislation. The GDPR entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant.[29]

The GDPR defines an array of legal terms at length. Below are some of the most important ones that we refer to in this article:

Personal data[30] is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. **Pseudonymous** data can also fall under the definition if it's relatively easy to ID someone from it.

Data processing[31], any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything.

[26] Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience*. OECD Publishing. https://doi.org/10.1787/02f0e5a0-en
[27] Council of Europe. (1950). *European Convention on Human Rights*. https://www.echr.coe.int/
[28] Council of Europe. (1950). *European Convention on Human Rights* art. 8. https://www.echr.coe.int/
[29] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 4(1)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[30] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 5*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[31] *General Data Protection Regulation (GDPR): Processing*. (n.d.). GDPR Info. https://gdpr-info.eu/issues/processing/

Data subject[32], the person whose data is processed. These are your customers or site visitors.

Data controller[33], the person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Data processor[34], a third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. These could include cloud servers, like Google Drive, Proton Drive, or Microsoft OneDrive, or email service providers, like Proton Mail.

In today's globalized economy, the transfer of personal data beyond the borders of the European Union (EU) has become an everyday necessity for multinational corporations.[35] However, the General Data Protection Regulation (GDPR) places stringent conditions on such transfers to ensure that EU residents' data enjoys an equivalent level of protection regardless of where it is processed. This regulatory approach is essential to uphold the trust of data subjects and maintain the integrity of EU data protection standards in an interconnected world.

GDPR provides a tiered framework for cross-border data transfers. At the forefront are adequacy decisions, whereby the European Commission evaluates whether a non-EU country's legal framework sufficiently protects personal data. When such adequacy is granted, data transfers proceed with fewer hurdles. Countries including Canada (specifically regarding commercial organizations), Japan, and Switzerland have been recipients of adequacy status, easing the compliance burden for corporations operating there.

However, securing adequacy is a complex process, often contingent on political negotiations and ongoing evaluation of the recipient's legal environment. Absent an adequacy decision, businesses must implement appropriate safeguards most commonly in the form of Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). SCCs are pre-approved templates that establish contractual responsibilities ensuring the protection of personal data during transfer3 These clauses bind both the transferring and receiving parties legally and

[32] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 4*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[33] *Data controllers and processors*. (n.d.). GDPR EU. https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/
[34] *General Data Protection Regulation (GDPR): Processing*. (n.d.). GDPR Info. https://gdpr-info.eu/issues/processing/
[35] Stoilova, V. (2021). *Regulation of international data transfers under EU data protection law*. CES Working Papers, 13(1), 1–16. https://hdl.handle.net/10419/286643

require thorough assessment to confirm that the destination country's surveillance laws or other factors do not undermine protection levels.

BCRs, on the other hand, enable multinational groups to self-regulate data flows internally, subject to approval from Data Protection Authorities, providing a holistic governance framework.4 In certain exceptional cases, GDPR permits transfers based on derogations, such as explicit consent from the data subject or the necessity for contract performance. However, these are designed as exceptions rather than the norm, given the legal uncertainty and increased compliance risk they carry.

The WTO Framework and Its Application to Cross-Border Data Flows

Origins and Limitations

The World Trade Organization agreements were negotiated during the Uruguay Round of trade talks from 1986 to 1994 and came into force on 1 January 1995[36] (Marrakesh Agreement Establishing the World Trade Organization, 1994). This timing is significant for understanding the limitations of the WTO framework[37] in governing digital trade: the agreements were concluded just as the commercial internet was beginning to emerge but before its transformative economic impact could be anticipated. As Dayday notes, "international trade law and the agreements forming the World Trade Organization (WTO) do not explicitly regulate digital trade and its different aspects, including cross-border data flows and data localization"[38] (Dayday, 2023: p. 33).

The WTO has recognised the growing importance of digital trade. In 1998, the Second Ministerial Conference adopted the Declaration on Global Electronic Commerce, establishing a temporary moratorium on customs.[39]

[36] World Trade Organization. (1994). *Marrakesh Agreement establishing the World Trade Organization*. https://www.wto.org
[37] Lopez-Gonzalez, J. (2025, October 13). *International trade and cross-border data flows* [PowerPoint presentation]. Organisation for Economic Co-operation and Development.
[38] Dayday, C. M. G. T. (2023). Cross-border data flows and data regulation under international trade law. *Philippine Law Journal, 96*, 33–81
[39] World Trade Organization. (1998). *Declaration on global electronic commerce (Ministerial Declaration)*. https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm

GATT Provisions and Their Applicability to Data as Goods

The General Agreement on Tariffs and Trade (GATT)[40] governs international trade in goods, establishing rules on tariffs, non-discrimination, quantitative restrictions, and exceptions to these obligations. As noted earlier, a threshold question in applying the GATT to cross-border data flows are whether data constitutes a "good" within the meaning of the agreement.

Several arguments support treating data as good under the GATT. Data has value, can be owned (through intellectual property rights), and can be exchanged between. Digital content, such as e-books, software, and digital media, shares many characteristics with physical goods that unquestionably fall within the GATT's scope.[41] Moreover, the WTO Appellate Body has previously recognised that electronically delivered content can be classified as a good, as in China—Publications and Audiovisual Products case, where it held that electronic distribution of audio-visual content fell within China's GATT commitments[42] (World Trade Organization, 2010: para 377).

However, counterarguments suggest that data may fall outside the GATT's scope. The ordinary meaning of "goods" arguably implies tangibility, which data lacks. The negotiating history of the GATT reveals no contemplation of intangible products like data. Furthermore, the existence of the GATS, which explicitly covers services delivered electronically, could suggest that electronic transmissions were intended to be regulated as services rather than goods[43] (Mitchell & Hepburn, 2018: pp 196-197).

If data is classified as "goods" under the GATT, several key provisions would apply to cross-border data flows. Article I[44] would require members to extend the Most-Favoured-Nation (MFN) treatment to data flows from all WTO members. Article III would prohibit discrimination between domestic and imported data (national treatment)[45]. Article XI would prohibit quantitative restrictions on data imports and exports, potentially capturing data

[40] World Trade Organization. (1994). *General Agreement on Tariffs and Trade 1994*. WTO
[41] United Nations Educational, Scientific and Cultural Organization. (2018). *Internet universality indicators: A framework for assessing internet development*. https://unesdoc.unesco.org/ark:/48223/pf0000262606
[42] World Trade Organization. (2005). *United States—Measures affecting the cross-border supply of gambling and betting services* (WT/DS285/AB/R)
[43] Mitchell, A. D., & Mishra, N. (2021). WTO law and cross-border data flows: An unfinished agenda. In M. Burri (Ed.), *Big data and global trade law* (pp. 83–112). Cambridge University Press.
[44] General Agreement on Tariffs and Trade 1994. (1994). World Trade Organization. Art. 1 https://www.wto.org
[45] General Agreement on Tariffs and Trade 1994. (1994). World Trade Organization. Art. 3 https://www.wto.org

localisation requirements and prohibitions on data exports[46]. Articles XX and XXI would provide exceptions for measures necessary to protect public morals, human health, and essential security interests, among other objectives.

The application of these provisions to data flows remains largely theoretical, as no WTO dispute has directly addressed the question of whether or not data constitutes goods. Nevertheless, the expansion of digital trade increases the likelihood that such questions will eventually require authoritative resolution, whether through dispute settlement or negotiated clarification among members.

CONSTITUTIONAL FOUNDATION OF PRIVACY AS A FUNDAMENTAL RIGHT

The flow of data across the borders, as discussed previously raises a serious concern regarding privacy and national security. This concern is not limited to one country only, it's for all the countries, worldwide. There are certain regional laws, as discussed, at international level to regulate and shape the global privacy standards, also ensuring the free flow of data across the borders, limiting the governmental interference, in the sensitive and personal data of the individuals, and restricting the use of personal data to an extent, and thereby forming the regulatory framework for the data protection.

The India's constitutional foundation for right to privacy and data protection, was established through the **Justice K.S. Puttaswamy v. Union of India[47] (2017) supreme** court judgement, wherein the court declared the right to privacy as a fundamental right under right to life and personal liberty[48] under Article 21 of the Indian constitution, intrinsically linked to the Article 14 and article 19[49]. This 9- judge bench ruling introduced a three-fold proportionality test requiring any privacy restriction to pursue a legitimate state aim[50], be rationally connected to that goal, and represent the least intrusive means.[51]

[46] General Agreement on Tariffs and Trade 1994. (1994). World Trade Organization. Art. 11 https://www.wto.org
[47] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, AIR 2017 SC 4161 (India).
[48] India. (1950). *The Constitution of India*, Article 21. https://legislative.gov.in/constitution-of-india/
[49] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597 (India).
[50] O'Brien, C. (2025, December 29). *Proportionality and reasoning in judicial review*. The Constitution Society. https://consoc.org.uk/proportionality-and-reasoning-in-judicial-review/
[51] Kakkar, J. M., Kaur, N., Aravindakshan, S., Mohan, S., Agarwal, S., Movva, S., Devadasan, V., & Bhandari, V. (2023). *The surveillance and digital governance landscape: A study of data, privacy, and state power*. Centre for Communication Governance, National Law University Delhi; supported by Global Network Initiative. https://globalnetworkinitiative.org/wp-content/uploads/2023/07/CCG-June-15.pdf

This acknowledgement of right to privacy has fundamentally led to the shaping of the cross-border data flow regulations like DPDP Act, 2023 and various other localizations in a fragmented way.

This chapter discusses the chronological order of the legislations and the regulations for cross-border data flows and India's stance of digital sovereignty.

Foundational Legislation: Information Technology Act, 2000 (Amended 2008)

The IT Act, 2000 provides India's digital backbone,[52] which highlights provisions regarding the data protection, privacy and cybercrime.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011[53]

This Rule is commonly known as IT Rule 2011, and the provisions relating to cross-border data transfer are an important aspect of the legislation, as they pertain to the transfer of extra-territorial personal data. These Rules are structured to ensure that the data rights of individuals remain protected even if their personal information is transferred to any other country. The IT Rule 2011 permits cross-border data transfer only if the destination country has a significant level of data protection mechanism. This means that the recipient country must be deemed to be at par with the standard set out in the IT Rule. If the recipient country does not have a satisfactory level of data protection framework, then the transfer of such information is only permitted if the individual has explicit consent to such

transfer (Rule 7), and Rule 641 IT Rule 2011 also requires organizations to disclose that personal data will be transferred internationally. This must be disclosed to the person before their data is transferred, and they must be informed of the potential risk involved in transferring their data to a country with fewer data protection laws. Overall, the provisions relating to cross-border data transfer under the IT Rule 2011 are designed to protect the data protection rights of individuals when data is transferred across the border. By outlining the conditions under which cross-border data transfer is permissible and security measures that must be taken, the

[52] Manupatra. (n.d.). *Information Technology (Amendment) Act, 2008: An overview*. https://articles.manupatra.com/article-details/Information-Technology-amendment-Act-2008-An-Overview

[53] Government of India. (2011). *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. https://www.meity.gov.in

IT Rule 2011 ensures that an individual's data is handled responsibly and according to procedures laid down in the legal structure. These safeguard an individual's personal information regardless of where it is being transferred.

Reserve Bank of India (RBI) Payment Data Localization (2018)

The Reserve Bank of India published and mandated, all payment system data must be stored in India, with transfers abroad requires prior RBI approval[54] (6 April 2018 circular). These directions were applicable to all the Payment system providers authorized/approved by the Reserve Bank of India[55] and were directed to setup the system under the Payment and settlement systems act, 2007.[56]

The data subject to the localization requirement includes full end-to-end transaction details, such as information collected, carried and processed as part of the payment instruction. [57] These provisions were to be strictly complied within six months of the circular, which profoundly re-shaped the India's financial technology ecosystem, the foreign trade and investment patterns, and global payment networks as well. The circular ensured that there is national sovereignty which meant that the state has the autonomy over the control on the data within the boundaries and the fintech industry has better localization laws, which required the data to remain within the domestic territory or imposed strict conditions on transfer, where the prior approval of the RBI is needed for the transfer of any sort of data internationally, till necessary.

The Digital Personal Data Protection Act, 2023 (DPDP Act)

The DPDP act, 2023 along with the Digital Personal Data Protection Rules, 2025[58] sets out India's new legal architecture for the processing[59] of digital personal data[60]. This framework

[54] Reserve Bank of India. (2018, April 6). *Storage of payment system data* (DPSS.CO.OD.No. 2785/06.08.005/2017-18). https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[55] Reserve Bank of India. (n.d.). *Frequently asked questions on digital payment systems*. https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995

[56] India. (2007). *The Payment and Settlement Systems Act, 2007*. https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=159

[57] Reserve Bank of India. (2018, April 6). *Storage of payment system data* (DPSS.CO.OD.No. 2785/06.08.005/2017-18).https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

[58] Press Information Bureau. (2025, November 17). *Digital Personal Data Protection (DPDP) Rules, 2025: A citizen-centric framework for privacy protection and responsible data use*. Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655

[59] India. (2023). *The Digital Personal Data Protection Act, 2023*, § 2(x). https://www.meity.gov.in

[60] India. (2023). *The Digital Personal Data Protection Act, 2023*, §§ 2(n), 2(t). https://www.meity.gov.in

also regulates the flow of digital personal data outside India. One of the most closely watched components of this framework has been the rule.[61]

The DPDP Act permits cross-border digital personal data transfer but there are certain restrictions being imposed. The Data fiduciaries, "means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."[62]

Processing of personal data outside India.[63] "The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified."

Data transfers under DPDP Act, 2023

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'.[64] 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 Parliament to enable scrutiny and allow for its modification or cancellation by the Parliament.[65]

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.[66] The contents of such a contract have not been outlined in the law. Neither does it mandate the government to issue

[61] Joshi, A., Nair, R., & Agrawal, B. (2025, December). *Cross-border data transfers under the Digital Personal Data Protection Act: What businesses need to know*. Economic Laws Practice. https://elplaw.in/wp-content/uploads/2025/12/Cross-border-data-transfers-under-the-DPDP-Act-what-businesses-need-to-know.pdf
[62]India. (2023). *The Digital Personal Data Protection Act, 2023*, § 2(i). https://www.meity.gov.in
[63] Government of India. (2023). *Digital Personal Data Protection Act, 2023* (Section 16). https://www.meity.gov.in
[64] Government of India. (2023). *Digital Personal Data Protection Act, 2023*, § 16(2). https://www.meity.gov.in
[65] Government of India. (2006). *Central Educational Institutions (Reservation in Admission) Act, 2006*, § 7. https://indiacode.nic.in
[66] Government of India. (2023). *Digital Personal Data Protection Act, 2023*, § 8(2). https://www.meity.gov.in

any rules or guidelines in this regard.[67] The DPD Act, however, makes it clear that the data fiduciary[68] would continue to remain fully responsible for compliance with the law in respect of any processing undertaken on its behalf by a processor.[69] 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.

Expiry of the retention period, and to cease processing the personal data of a data principal if they withdraw their consent.[70] 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.[71] 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 meet 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. Considering 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.[72] 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.[73] 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.

[67] DLA Piper. (2026). *Data protection laws of the world: India*. https://www.dlapiperdataprotection.com/?t=law&c=IN
[68] Government of India. (2023). *Digital Personal Data Protection Act, 2023*, § 2(i). https://www.meity.gov.in
[69] Government of India. (2023). *Digital Personal Data Protection Act, 2023*, § 8. https://www.meity.gov.in
[70] Government of India. (2023). *Digital Personal Data Protection Act, 2023*, § 8(7). https://www.meity.gov.in
[71] Government of India. (2023). *Digital Personal Data Protection Act, 2023*, § 11(1)(b). https://www.meity.gov.in
[72] Government of India. (2023). *Digital Personal Data Protection Act, 2023*, § 17(1)(d). https://www.meity.gov.in
[73] Ministry of Finance, Government of India. (2023). *Budget 2023-2024: Speech of Nirmala Sitharaman, Minister of Finance, February 1, 2023*. https://www.indiabudget.gov.in/doc/bspeech/bs2023_24.pdf

CONCLUSIONS AND RECOMMENDATIONS

The comprehensive legal analysis of cross-border data flows and digital sovereignty reveals a complex global landscape where economic interdependence collides with national security imperatives. The EU GDPR has established the equivalence principle as the international gold standard, conditioning transfers through rigorous adequacy decisions, Standard Contractual Clauses supplemented by Transfer Impact Assessments, and a robust proportionality doctrine rooted in fundamental rights protection. In parallel, WTO GATS disciplines and modern preferential trade agreements like CPTPP and USMCA prioritize free data flows through market access commitments, carefully tempered by exceptions that demand necessity and non-discrimination tests. OECD soft law instruments and APEC Cross-Border Privacy Rules foster essential interoperability, while India's Digital Personal Data Protection Act Section 16 exemplifies strategic autonomy authorizing default free flows for non-critical data while maintaining sovereign control over strategically important categories, all grounded in the constitutional privacy framework established by Justice K.S. Puttaswamy (2017).

The conflicts are stark and multifaceted. China's Data Security Law and Personal Information Protection Law impose comprehensive localization that fragments global supply chains, the Schrems II/III saga exposes fundamental tensions between US CLOUD Act extraterritoriality and EU Data Act resistance mandates, and India's RBI 2018 payment data localization at an estimated $8 billion compliance cost demonstrates how sovereignty measures reshape entire fintech ecosystems. These competing interests pit massive $3 trillion annual GDP gains from frictionless flows against legitimate privacy, security, and economic protection concerns that no responsible state can ignore.

International organizations provide critical coordination WTO's Joint Statement Initiative, OECD's Global Privacy Enforcement Network, APEC CBPRs, and UN's Global Digital Compact but lack binding enforcement authority. India emerges as a pivotal case study, the global expansion of UPI (15 billion monthly transactions reaching France and UAE by 2026) proves data flows drive economic growth, while Aadhaar's strategic siloing protects core sovereignty interests.

The central thesis of this analysis stands confirmed, proportionality requiring legitimate aims, rational connection to those aims, and adoption of the least intrusive means serves as the unifying principle capable of reconciling the hard law disciplines of GDPR and WTO, the soft

law harmonization of OECD, and constitutional frameworks like India's Puttaswamy doctrine.

11.2 The Proportionality Imperative

Proportionality emerges not merely as a legal test but as the foundational architecture for sustainable data governance. Blanket localization mandates like China's critical infrastructure operator requirements fail this test by imposing disproportionate trade barriers that exceed security necessities. Conversely, pre-Schrems unrestricted flows exposed unacceptable vulnerabilities to foreign surveillance. The balanced "default permission + targeted exceptions" model exemplified by India's DPDP Section 16, USMCA Article 19.1, and OECD Guidelines Articles 16-17 satisfies all three prongs: legitimate privacy/security aims, rational connection through risk-based classification, and minimal intrusion via permission-by-default regimes.

India's RBI 2018 guidelines passed constitutional muster by permitting data mirroring rather than hoarding, providing six-month transition periods, and demonstrating clear fraud prevention benefits. China's comprehensive mandates, by contrast, struggle against WTO Article XIV necessity requirements, while US FISA Section 702 bulk collection lacks adequate safeguards against overreach.

11.3 Strategic Policy Recommendations

11.3.1 <u>Multilateral Framework Development</u>

The international community must prioritize tiered harmonization over universal standards. WTO Members should integrate the Joint Statement Initiative on E-commerce texts as a plurilateral agreement by the 2028 Ministerial Conference, incorporating OECD proportionality benchmarks for legitimate public policy exceptions. The European Data Protection Board and OECD should collaborate on a Global Transfer Impact Assessment template by 2027, harmonizing Schrems II requirements with APEC CBPR accountability frameworks to reduce compliance duplication.

Sectoral adequacy decisions, healthcare data following WHO standards, financial data aligned with BIS frameworks offer pragmatic mutual recognition paths. Bilateral memoranda of understanding between high-flow partners (India-US, EU-Singapore, Japan-Australia) can serve as immediate trust-building measures while multilateral negotiations mature.

11.3.2 National Policy Reforms

India should implement three-tier data classification in finalizing DPDP Rules 2026: public interest data (free flow), normal personal data (default permission), and genuinely critical data (prior permission). China could introduce risk-based exemptions for fully anonymized analytics datasets, preserving security while enabling AI research. The European Union should establish safe harbor presumptions for Data Privacy Framework-compliant US firms pending Schrems III resolution. The United States must strengthen judicial oversight mechanisms for CLOUD Act warrants involving foreign nationals' data.

For India specifically: RBI should permit federated analytics on anonymized payment data to restore real-time fraud detection capabilities, while MeitY pursues APEC CBPR certification to facilitate UPI Stack global exports.

11.3.3 Technological Solutions

Technology offers sovereignty-preserving alternatives to geographic localization. Homomorphic encryption enables computation on encrypted data without decryption, federated learning permits collaborative AI model training without raw data transfer, and zero-knowledge proofs verify compliance without substantive disclosure. G20 Digital Economy Ministers should endorse a "Sovereignty Tech Stack" with ITU standardization targeted for 2028, positioning these privacy-enhancing technologies as legitimate alternatives to data residency mandates.

11.3.4 Capacity Building for Global South

Technical assistance programs must address enforcement capacity gaps. European Data Protection Authorities should train India and Brazil's data protection boards on adjudication and DPIA methodologies. OECD should extend TIA training to ASEAN economies, while Singapore CERT builds African cybersecurity response capabilities. India's India Stack Aadhaar, UPI, Account Aggregator should be packaged as an open-source digital public infrastructure export model for Global South adoption.

11.4 Implementation Roadmap and Risks

A five-year roadmap charts the path forward: 2026 establishes global TIA standards and

expands APEC CBPR membership; 2027 sees WTO JSI plurilateral entry into force and India's tiered adequacy system; 2028 integrates JSI disciplines into WTO framework alongside Sovereignty Tech Stack standards; 2029-2030 focuses on sectoral harmonization to unlock the $5 trillion digital trade potential.

Inaction risks catastrophic fragmentation: US-China parallel internets could cost $2.5 trillion in foregone trade, EU adequacy fatigue breeds SCC proliferation and enforcement chaos, while Global South competing localization regimes stifle development. ECIPE conservatively projects $1.6 trillion annual digital trade suppression by 2030 absent harmonization.

11.5 Vision for 2030 Data Governance

The sustainable path envisions a rules-based global digital order where 85% of cross-border flows operate under mutual recognition arrangements, proportionality serves as the universal balancing mechanism, India leads the Global South through digital public infrastructure exports, and sovereignty evolves from geographic control to governance capacity. Data flows become sovereignty's enabler rather than existential threat.

Conclusion

Without proportionality-based multilateralism operationalized through tiered adequacy, global TIA standards, and tech-neutral implementation, digital balkanization becomes irreversible. With determined leadership particularly from digital middle powers like India cross-border data flows can power inclusive global prosperity while respecting legitimate sovereignty concerns.