LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

SECURING BORDERS IN CYBERSPACE: QUEST FOR DATA SOVEREIGNTY AMIDST GLOBAL TRADE, HUMAN RIGHTS AND CROSS-BORDER PRIVACY CONCERN

Dr. Roshni Shrivastava[1], Aniket Dwivedi[2], Gautam Jaiswal[3], Shivangi Gupta[4], Dr. Kulsoom Ruma[5]

[1]Associate Professor, Amity University Lucknow, Orcid Id: (0009-0002-3407-6698)
[2]Research Scholar, United University
[3]Research Scholar, United University
[4]Assistant Professor, Balaji law College Pune
[5]Assistant Professor United University Prayagraj

roshnishrivastava09@gmail.com[1]
dwivedi911846@gmail.com[2]
jaiswalgautam4@gmail.com[3]
shivangigupta976@gmail.com[4]
rumah.farooqui@gmail.com[5]

Abstract
In a rapidly changing world where actions and movements are influenced by digital interdependence, the 'national' sovereignty has changed from a physical view of borders to that of control over data generated, stored, and utilized in a national territory. India, as an emerging digital power, is in the position of championing sovereign data rights while also complying with transnational trade rules that call for the free flow of data in and out of borders. This paper reviews India's emerging position defending its digital borders, as it supports the localized governance of data, creates an integrated body of laws, and influences statements by the public sector. It makes clear the country is driven by national security interests, economic independence, citizens' informational privacy, and how it manages these tensions while complying with the conditions of international trade and multilateral digital partnerships. It is an exploration of the tensions between domestic policy agendas and external economic imperatives, and places India's assertions of data sovereignty into a larger global context. Through the analysis of strategic documents, recently passed legislation like the Digital Personal Data Protection Act, and India's representations in international fora, this study defines both the possibilities and challenges for India to fulfil its digital sovereignty ambitions. In closing, we offer suggestions on how India can build its sovereign digital future while its responsibilities to international data interoperability and global connectivity shown using a combination of different opportunities, without compromising its flexible, strategic data rights.

Keywords*: Sovereign Data, Digital autonomy, Data localization, Cyber Data colonialism, Digital Sovereignty, Cross-border Privacy*

Introduction

The world which we will live in is inseparably connected with the digital world we nowadays communicate with. Because our physical and virtual lives are getting more and more integrative, this offers us a special chance to improve our lives. The relevance of sharing data has been highly valued in the last several decades and provides great opportunities to foster social life integrity as well as financial welfare. The adoption of such digital transition can give rise to some new solutions, making our lives better. Numerous fields in the sphere of economy have experienced innovations because of data transfer, and international exchange of data enhances the relationships between nations as well. Nonetheless, several problems regarding the

management of data, such as the location of data, means of accessing data, and processing data are accentuated by this sudden rise in the cross border communication of data. Data sovereignty is the notion that data comply with rules and regulations of a country.[1] This implies that countries can control and dictate the information generated within their territories including its transfer as well as its storage. In response to the diversion of the flow of data across national boundaries, policies and regulations relating to data safety have been enhanced ensuring that their data remain in their own borders, or at least, in their custody. Cross-border data flows refers to data transfer between countries typically within the context of online services and data analytics or global corporate operations. Such flows are important to the functioning of the global economy as they provide companies with access to foreign markets and also to aid supply chain. They provide the client with assorted online services which are available regardless of their position.[2] There are challenges to cross-border data flows though. The laws involving the security and privacy of data differ according to each country, and this further increases the complexity of the problem to businesses. As far as the sphere of digital government is concerned, transboundary data transfer is a crucial aspect of the efficient cross-border transfer of sensitive or personal information. These transfer helps the different positive projects such as the improvement of government services, enhancement of international partnerships, and promotion of data sharing between the government and non-government organizations. Due to this ideology, much can be done to enhance services provided by government and promote international collaboration. The virtual world that we live in nowadays is key to re-shaping a promising future. We are utilizing the virtual world more and more, and therefore, the border between the real world and the virtual one is becoming thinner. This changing world shows the increasing significance of data transfer on social development and economic success. With such opportunities, we are able to achieve a more unified and cooperative world. In the contemporary digital environment, transboundary data transfers are the major factor which defines the operation of the digital government. This is a process through which sensitive or personal information moves across national boundaries to many purposes that are critical; some of the reasons are the provision of governmental services, the development of international partnerships, and data sharing occurred between government agencies and the corporate communities. The importance of the cross-border data flow is impossible to overestimate; it is the definitive building block of improved governmental services and a stimulator of international collaboration. This is not only a significant approach but also the key that will spur innovation and enhance the living standards of the citizenry across geographies in face of an increasingly interconnected world.

The world will certainly belong to the digital future and the difference between the virtual and the real world is quickly fading. Data exchange is also proving to be a decisive element towards creating social and economic prosperity. The adoption of transboundary data transfer is not only a strategic decision to be made, it is the need of governments that want to prosper in the 21st century.[3] In this paper, it is categorically stated that data privacy as a basic right needs protection. It will carry out a critical review of the privacy laws of India to draw important areas to be

1 R. Baldoni & G. Di Luna, *Sovereignty in the Digital Era: The Quest for Continuous Access to Dependable Technological Capabilities* (2025)

2 M. R. P. — *Regulating Cross-Border Data Flows: Issues, Challenges and Impact* (Anthem, 2024)

3 Atlantic Council, *India's Data Localization Pivot Can Revamp Global Digital Diplomacy*

protected. Moreover, although there are certain legislations designed to secure the personal data, in many countries the effective legislation still remains a problem because of the absence of the common legal regulation. This can very well depict the dire need of such an international system to manage cross border data transfers. It is critical that, in order to facilitate the internet openness and valuable consumer and corporate faith, the World Trade Organization (wto) needs to rewrite its regulations in order to establish the legislative problems of the data-driven economy. In this analysis, the research author has divided it into five sections to adequately address the areas of concern. The first one is simple introductory text, In the second part, we claim the increasing significance of the subject. The third corner covers the cross-border data transfer and focuses on how it can boost economic growth and contribute to flourishment of innovative services that are crucial in enhancing the process of global digitization.
The fourth part is really a hard analysis of the issues and problems related to the free transfer of the cross-border data such as the privacy protection of the data and the necessary balance between the data sharing and privacy as well as national security. This part goes through the legal systems in India which deal with the issue in question.

Significance of the study

IPRs are becoming more and more significant in the economy. Progress of nations IPRs guarantee the preservation of exclusive exploitation rights, which is necessary for future technological growth. Patents granted by the nations and each have its own set of laws. India had seen firsthand how the British had created the Patent Act of 1911 and then repealed the previous legislation to create its own Patents Act of 1970, which was more suited to local growth. Many developing nations, including India, were compelled to ratify the TRIPs agreement in sort to harmonize the patent structure due to pressure from the industrialized world. The TRIPs regulations compliance was of utmost importance, and India had complied. Since the Uruguay Round talks were underway and TRIPs was being discussed, there has been a tremendous clamor for change heard all across the world. One section continues to be a critique while the other justifies patent regime. The current study will concentrate on how the Amended Indian Patent Act complies with the TRIPs standards and what implications it has for the Indian economy and future prospects. IPRs have been a hotly disputed topic for the past two decades due to the TRIPs, and several research, seminars, and conversations are being held to raise awareness of the issue. Additionally, the bulk of Indian colleges offered IPRs as a stand-alone diploma subject in addition to conventional courses. The current topic has been chosen for the study in light of the growing significance of the subject.

Human Rights in the Age of Data Sovereignty:

Cyberspace an interconnected area that transcends national borders and promotes global communication trade innovation and governance has emerged as a critical area of human interaction in the twenty-first century. But traditional notions of state sovereignty have also been muddled by this digital interconnectedness leading to contentious debates over who has jurisdiction over the flow of data information and digital infrastructure. As nations struggle with privacy concerns international data transfers and cybersecurity threats pursuing data sovereignty has become a major issue in modern international law and governance. In the past territorial control—the supreme authority of a state within its borders—was thought to be the essence of sovereignty. Cyberspace however is not limited by geography data stored on cloud servers

which are often located outside of national borders moves between continents in milliseconds. This technological environment has led to a complex web of moral legal and political issues. Who owns the information generated in a country? Who can process store or analyze it? What roles do businesses and governments play in protecting the fundamental rights of people whose information is at risk? The human rights component is at the heart of this conversation. Data represents peoples actual identities including their behaviors beliefs preferences health information and interactions. It goes beyond simply being a commercial asset or an essential part of the digital economy. The rights to privacy and human dignity are directly violated by any inappropriate use or unapproved monitoring of this data. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights both declare privacy to be a fundamental human right that applies to both digital and offline contexts. In its landmark Resolution 20/8 (2012) the UNHRC affirmed that the same rights individuals possess offline must also be safeguarded online. . This recognition emphasized the need for technological advancement to operate within the moral bounds of human rights. In addition to improved cybersecurity measures the digital age calls for an ethical framework that guarantees technology advances humanity rather than subjugates it. Actually the digital world has become a battleground for three main forces: governments trying to protect national security companies seeking to make money using data-centric models and individuals trying to preserve their privacy and autonomy. There is a delicate balance between these interests. On the one hand officials argue that data regulation is necessary for national security cybersecurity and counterterrorism reasons. Multinational corporations on the other hand support open data movement in order to promote global innovation and trade. Many times in this struggle people become passive objects and their data is used for commercial purposes without their actual consent. This tension is exemplified by India own journey. With more than 800 million internet users the country faces major challenges in protecting data integrity and privacy making it one of the largest digital economies in the world.

India attempt to strike a balance between economic priorities and individual rights is reflected in the Digital Personal Data Protection Act (DPDP) (2023). Inspired by Justice K. A. Puttaswamy versus Union of India (2017) decision which recognized privacy as a fundamental right under Article 21 of the Constitution the DPDP Act represents a major advancement in both constitutional law and policy. It emphasizes the significance of consent purpose limitations and data reduction while giving the government significant power to uphold compliance and oversight. From a legal philosophical and human rights perspective the rest of this paper examines these issues emphasizing that future cyberspace governance should be founded on a human-centered digital framework rather than just a nationalist or economic one.

Data sovereignty: Sovereignty, Security, and Surveillance

Data sovereignty refers to the notion that information gathered with the territory of one nation falls under the control of that country and cannot be subjugated by any other nation. The idea is that the data has a nation place to call home. It is under the jurisdiction of the rules and regulations of the country that it is harvested and refined in. According to the concept of indigenous data sovereignty, a country is entitled to regulate the collection, ownership and utilization of data of its very own. In the digitalized age, data sovereignty is now gaining more and more attention as data generation and gathering in myriad avenues is growing not only in social media; mobile devices, e-commerce markets, and even in the digital world as a whole,

Governments are deeply interested in protecting corporate and personal information as well as have some control on the data that have an impact on national security. As a result, issues of sovereignty and data localization are also becoming popular in the more sensitive set of issues on cross-border data flow. Most countries are contemplating or already had enacted data localization policies by which they want particular kinds of information to be stored on their soil, signifying their concern in safeguarding information of their people. The idea of India living in the era of digital colonization or a data colonialism (unrestricted flow of data in and out of India to the Western nations and other countries) sounds serious in terms of national security and privacy of the individual.[4] People can now exchange information more easily across national borders due to the global nature of the internet, which promotes the spread of malicious AI-generated content, most notably deepfake, since they threaten their privacy and dignity. Regulation of DPDPA (Section 16 (1) enables blacklisting of countries which threaten national security or privacy of the people. This can be ruled out by the fact that breaches of data may be initiated by commercial businesses, social media entities and techno-defense organizations that are based in a variety of countries.[5]

The data privacy must not be utilized as a weapon to attack the cyber-surveillance and intelligence apparatus of nations. But the trick is to ensure that data privacy does not take the form of a diplomatic move. Taking a look at one of the events in June 2020, when The New York Times covered the unceremonious removal of Chinese applications by India as a threat to national security and sovereignty, one might arrive at a conclusion that such a measure might be the result of the previous border conflicts."

Businesses also consider data sovereignty; those entities that have business within the country must comply with its laws and regulations on data protection. This means that they must ensure that information generated and collected internally is processed and kept within the laws of the region. Violation of such rules might have both financial and legal consequences. Data sovereignty enables companies to own the data and assure that it cannot be accessed or stolen by unauthorized third parties.

Causes of elevating data sovereignty:

The causes of elevating data sovereignty as a serious issue are:

- **National security:** On a security point of view, governments are always in concern on how to protect data which is assumed to be sensitive. This is most urgent in case of defense, intelligence and data pertaining to critical infrastructure where there is high probability of occurrence of cyber-attacks.
- **Data protection and privacy:** With more and more digital platforms, exploitation of data and the increasing number of cybercrimes are making their entry and various countries are crafting data protection laws to ensure the privacy of their citizens.
- **Political and ideological issues:** Data sovereignty can be affected by political ideology as well. Some governments are attempting to have greater control over the information in order to maintain the status quo and adhere to cultural values.

Cross-border data transfer

4 MP-IDSA, *Data Protection Frameworks of India and the US: Data Sovereignty vs Market Flexibility* (2025)
5 *Draft data rules introduce potential for data localisation requirements"*, ET, June 2025

In an impressive collaborative effort, leading cloud service providers have banded together to enact the "Trusted Cloud Principles", a significant commitment to achieve the best possible security and privacy for customer data across borders. An important component of this framework is that it recognizes the important role for government assistance in enabling data sharing over borders, which is an important enabler for innovation, efficiency, and security, and enthusiastically endorses the removal of restrictive data residency laws. The simple truth is that the traditional concept of borders is fading in an increasingly digital world. There is an emerging recognition that using data more freely across borders is an important catalyst for online commerce and economic growth. To harness this opportunity, it is vital for governments to enact laws that protect people's privacy and personal data and also encourage the free flow of information across borders. These two conditions will create an environment where innovation can flourish and positive economic outcomes will flow to the masses. In an increasingly digital world, where our lives are becoming more interconnected across borders, leading cloud service providers have created the "Trusted Cloud Principles."[6]

We are committed to delivering this message to protect the privacy and security of your data, wherever you happen to be in the world. The cornerstone of these principles includes understanding that governmental assistance to support international data sharing is needed; this sharing of all personal data allows substantial growth in innovation, efficiency, and security while also opposing barriers to data residency. This is a time when the lines associated with national borders are growing blurry; this both opens new windows and creates hurdles. Expanding cross border data sharing expands online commerce and engenders economic opportunity for everyone; data flows create a multiplier effect financially. It is vitally important that governments design laws that protect your privacy and personal data, while also encouraging an open exchange of data. Together we can create a safe and robust digital landscape that cultivates your rights and opportunity. The unmistakable connection between cross border flows of data and other international trade illustrates how critical data transmission has become to the incredible rise of global commerce. It is difficult to imagine a global business transaction today that does not involve the exchange of data. To maximize the potential between the two, legislators need to craft a reasoned legislative pathway for data to flow across borders.[7]

As the exchanges of global data continue to grow, the focus on creating strong regulations will help address significant issues such as privacy, data protection, and national security. By implementing strong protections surrounding personal data exchanges, we can create a safe surrounding that prevent abuse and enable responsible usages of data, and help support success of the economy. There are a number of important regulations, including the General Data Protection Regulation (GDPR) in the EU, APEC Privacy Framework and Privacy Shield Framework between US and EU that give bodies the ability to proceed with secure cross-border data transfer. However, any company that will manage personal data of EU citizens (irrespective of its location) is expected to comply with GDPR. This is a robust framework that provides protections for the individual privacy and establishes the highest standards for data transfer, along with outlining the responsibilities of the businesses that are operating in the global marketplace. Compliance with these regulations is not simply a legal requirement; it is an essential commitment to protecting personal data and building trust with its customers

6 *India's stance on data transfers at WTO spooks chip giants"*, Reuters, Feb 2024
7 *The Line Between Digital Trade and Security Is Always Blurry"*, Wired, 2021

worldwide. The Digital Personal Data Protection Act of 2023, called the DPDP Act, lays down definitive regulations on the export of personal information from India. Section 16 of this Act certainly speaks to cross-border data transfers, and speaks to the numerous critical issues
Section 16(1) gives the Union government the express privilege of restricting personal data anywhere in the world, by the named countries to which the restriction applies, by notice (and ultimately it may be seen that such restriction could cover any country where notice is given).
Section 16(2) obviously ties back to existing laws, allowing for present and effective data protection measures.16 Section 43A of the IT Act provides similar protection for sensitive personal data. It should be noted that at present India does not have a national, or sector specific regulatory body to oversee the protection of personal information in India. India continues to lead any discussion globally in the worlds of Information Technology (IT) and business process outsourcing (BPO), with projected predictive analysis estimating that this fast-growing industry will produce a remarkable 8% to India's growth.
Additionally, in order to fulfil legal requirements, data fiduciaries in India can share personal data with the State or its agents without consent from the concerned party. This is a recognized lawful basis for the use of data allowing its use for the greater ease of governance while providing the State and its agents some safeguards.14 Furthermore, the State and its agents can process personal data for legal purposes and for the purposes of maintaining national security, sovereignty and public order without obtaining consent and certain obligations under the DPDP Act. While this exemption poses some democratic hurdles for EU exporters analyzing the implications of the Schemes II decision impacting data transfers to India, it also provides a starting point for discussion on how different regulations will be construed.15 In addition, the Board responsible for upholding proper protection of personal data is made up of individuals, including a chairperson appointed by the Indian government in accordance with the DPDP Act. Interestingly, unlike the GDPR, the DPDP Act specifically establishes a scheme of sanctioning violation and non-compliance that does not depend on the revenue of the body. This model may potentially stimulate a more flexible atmosphere for compliance and accountability in the processing of personal data.[8]
The DPDP Act lays out a scheme of fines that vary significantly in their terms, ranging from INR 50 crores to 250 crores (roughly 5 million to 25 million euros), for certain offenses. Unlike previous versions of the Act, the Act does not set maximum fines for many offenses; such as for example, a failure to set security measures, and the duty to notify the Board after a data breach. Instead, there are specific penalties for each offense and therefore it allows those to be recombined to derive a maximum on total penalties.

Guarding the data: The Politics of Digital Control

Data is an incredibly valuable asset that covers everything from an entire country's population data to personal information about citizens and exclusive information from governments. In the digital era, data is valuable, but demand protection. Data can be viewed as gold, but it should be recognized for what it is - it can be attacked by cybercriminals using sophisticated artificial intelligence. Data can be compromised and pose serious privacy threats to organizations and individuals. If we can secure data and allow it to thrive, the possibilities are endless.

8 Atlantic Council, *India's Data Localization Pivot Can Revamp Global Digital Diplomacy*

Safeguarding data will protect the ability for it be used but done responsibly. Let us provide a better and safer world.

In the current digital landscape, crimes have evolved into online crimes that may threaten secure cyberspace. Therefore, for effective ways to combat them, secure frameworks for data privacy should be created. But in order to create secure frameworks for data privacy, the Puttaswamy judgment (2017) formed a strong basis for privacy consciousness, and it set the atmosphere for concerning the importance of privacy in the digital world. It is also interesting to note that the digital world represents a little more than national border, an important concept I will refer to as cross-border data transfer. This is where data is transferred across territorial borders, or data is transferred between jurisdictions. In particular, Section 16 of India's data privacy law regarding Digital Personal Data Protection Act, 2023 (DPDPA) provides useful (indirect) guidance for proper management involved with cross-border data transfers and to ultimately provide a safe and secure online world. For instance, subsection 1 allows data to be transferred to any country minus those that the central government lists as being on the 'blacklist'.[9] By enacting legislation, the government has tackled an issue by balancing data privacy with the economic development, and as opportunity promotes growth, we can expect sector specific legislation, as provided in section 16(2), that balances opportunity for sector based economic growth with data privacy. While the legislative framework will likely be a step in the right direction, it also exposes opportunities to address existing issues concerning cross-border data transfer absent in the DPDPA, thus improving the regulation.[10]

Conclusion

Privacy should not be a trade off for being online. The Indian IT regime must take proactive steps towards protecting digital data and supporting its free flow. The overriding question is: can we trust that data will be safe in the existing architecture and post-transmission. The government must have a strong policy in place. Individual rights to informational privacy must be guaranteed by having stringent legislation over the movement of data across borders and it must be illegal for people to deceive or hurt individuals with cybercrimes or malfeasance in general. The global digital economy is currently assessed at more than $15 trillion. Nations promoting data localization contend that keeping and managing data within their borders provides enhanced regulatory oversight and strengthens national security. India’s DPDP Act empowers the central government to set regulations for cross-border data transfers, ensuring continued oversight.

Finally, data sovereignty and cross-border data flows are some of the very few pressing issues today for the international digital economy. Businesses become more global and nations more connected economically and socially, we face challenges reconciling the imperative of unrestricted data flow and the interests of countries in exercising legitimate national data sovereignty and national security interests and the rights of individuals and corporations to restrict processing and storage of their data and private information within the borders of their own nations. Data sovereignty means that sensitive data is processed and stored in the country of origin to mitigate risks of exposure and compliance with national regulations and local legal

9 Official Gazette Notification (Full DPDP Act PDF) https://egazette.gov.in/WriteReadData/2023/248045.pdf
10 https://www.snrlaw.in/wp-content/uploads/2023/09/SR-Data-Indias-New-Law-The-Digital-Personal-Data-Protection-Act-2023.pdf

protections. Unfortunately, this is a hindrance to a free flow of data across borders - which is vital for global enterprises, innovation and economic development. In conclusion, the future of data governance will depend on active global collaboration and the development of broad global privacy and data protection standards. We need a legal framework that strikes a balance between national sovereignty and the obligation to protect data.

As a significant player in technological service outsourcing, India is writing a data privacy law that will heavily influence cross-border data flows. The study that was recently published by the joint parliamentary committee on the Personal Data Privacy Bill, 2019 illustrates that companies will incur significant risk if they transmit sensitive personal data to any country, regardless of whether that country has strong data privacy laws. The bill permits the cross-border transfer of a large amount of personal data under intra-group transfers, including legal obligations based on corporate regulation or approved standard contractual arrangements from the data protection authority. It is important to clarify the level of restrictions that have been placed without delay. The international flow of data is increasingly at risk due to ongoing restrictions concerning data localization.

The e-commerce policy proposed for India has faced fierce opposition, primarily for similar grounds. In our world of increasing connectivity, it is critical that we clarify the frontiers of data sovereignty through more assertive policymaking. The legal fiction on the cross-border transfer of data is rapidly evolving, and courts need to more aggressively reconcile the fundamental right to privacy and data protection with other legitimate public and commercial interests so as to establish meaningful and minimum standards. The rapidly changing nature of technology, including artificial intelligence, cloud computing, and sensors in the Internet of Things is throwing new challenges into the mix. It is important to have more focused conversations among stakeholder's state actors, business, technologists, civil society and international organizations if we are to agree on effective solutions. Cross-border transfer of data raise important questions concerning the limits of corporate power and individual liberties as well as state sovereignty in an increasingly interconnected world. It is important to balance these conflicting interests if we are to create common standards. Getting the balance right between protecting the public interest and extracting the enormous economic and social benefits from cross-border data flows is not only necessary but can be expected for our future generations.

REFERENCES:

- R. Baldoni & G. Di Luna, *Sovereignty in the Digital Era: The Quest for Continuous Access to Dependable Technological Capabilities* (2025)
- **Official Gazette Notification (Full DPDP Act PDF)** https://egazette.gov.in/WriteReadData/2023/248045.pdf
- https://www.snrlaw.in/wp-content/uploads/2023/09/SR-Data-Indias-New-Law-The-Digital-Personal-Data-Protection-Act-2023.pdf
- Atlantic Council, *India's Data Localization Pivot Can Revamp Global Digital Diplomacy*
- India's stance on data transfers at WTO spooks chip giants", Reuters, Feb 2024
- *The Line Between Digital Trade and Security Is Always Blurry"*, Wired, 2021
- *Draft data rules introduce potential for data localisation requirements"*, ET, June 2025