Page 1181 - 1192 **DOI:** *https://doij.org/10.10000/IJLMH.119782*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Data Sovereignity vs Data Globalistaion: Legal Dilemmas in an Era of Digital Borders and Borderless Data

SHONEZI FATIMA[1]

ABSTRACT

In the digital age, the clash between data sovereignty and data globalisation has become one of the most pressing legal and policy challenges facing governments, businesses, and individuals. This paper is a research exploration of the escalating legal tensions between data sovereignty and data globalization in the digital era. As an increasing number of countries implement laws to regulate data generated within their jurisdictions, issues surrounding national security, privacy, and public interest have prompted the introduction of stricter regulations, such as the European Union's General Data Protection Regulation (GDPR), China's Personal Information Protection Law (PIPL), and India's Digital Personal Data Protection Act (2023). Concurrently, the contemporary global economy relies significantly on the seamless flow of data across borders, which is essential for cloud computing, digital trade, and online services.

This interdependence creates substantial legal challenges, particularly when national laws conflict or when disparate standards are applied in cross-border situations. For instance, the GDPR imposes stringent requirements on data handling that may clash with less rigorous regulations in other jurisdictions, leading to complications for multinational companies operating in diverse legal environments. The paper explores these complexities through doctrinal legal research, comparative analysis, and selected case studies, including Schrems II and the Microsoft Ireland case. Additionally, it examines how trade agreements such as the USMCA and CPTPP attempt to address these tensions. Furthermore, the discussion encompasses broader issues like digital inequality and data colonialism, highlighting how disparities in data governance can exacerbate existing inequalities between nations and within societies. The paper argues that without careful consideration of these factors, the push for data sovereignty could lead to a fragmented digital landscape that hinders innovation and economic growth. The discussion also encompasses broader issues like digital inequality and data colonialism, ultimately offering recommendations for more balanced and collaborative legal frameworks. The aim is to identify strategies that safeguard national interests and individual rights while fostering global digital innovation.

[1] Author is a Law Graduate in India.

 [ISSN 2581-5369]

Keywords: *Data Sovereignty, Data Globalization, Digital Age,General Data Protection Regulation (GDPR), Digital Personal Data Protection Act (2023), Legal Challenges.*

I. INTRODUCTION

With the world becoming more data dependent, countries are realizing the importance of data sovereignty. As data increasingly becomes a cornerstone of economic activity, political governance, and personal autonomy, the question of who holds control over this data, and under which legal frameworks, has emerged as a critical issue. This dynamic is encapsulated in two contrasting paradigms: data sovereignty, which posits that data is governed by the laws of the nation where it is collected or stored, and data globalization, which advocates for the unrestricted flow of data across borders as essential for innovation, efficiency, and economic integration.

Sovereignty means the exclusive and supreme authority of a state without any internal competitors or external influence. Data sovereignty is a term that underlines the nation's ability to control its own data, ensuring that the stored and processed, protected in accordance with its laws an regulation. States often invoke this notion to impose restrictions on data flows, citing reasons such as national security, privacy protection, or economic self-determination. Conversely, data globalization reflects the borderless nature of the internet and the needs of transnational commerce, where multinational corporations, cloud computing, and cross-border services depend on the unhindered movement of data.

This legal tension presents significant challenges for international digital governance. Divergent regulatory frameworks, such as the European Union's General Data Protection Regulation (GDPR), the fragmented sectorial approach of the United States, and China's cyber security and data localization laws, illustrate the growing differences in national data governance strategies. Meanwhile, international trade agreements strive to bridge these gaps by promoting cross-border data flows under specific safeguards, though often with limited effectiveness.

In this context, this research paper seeks to address the central question: How can legal systems reconcile national control over data with the inherently global nature of digital networks? The study will explore the conflicts between privacy rights, commercial interests, and claims of digital sovereignty. These conflicts are not merely theoretical; they manifest in high-profile legal disputes and policy decisions that have far-reaching implications for global markets and fundamental rights.

 [ISSN 2581-5369]

Employing a doctrinal legal methodology, this research will draw on primary legal sources, including legislation, judicial rulings, and international agreements. A comparative analysis will be conducted to contrast the approaches of key jurisdiction-primarily the EU, United States, China, and India, highlighting both areas of convergence and divergence. Case law analysis, including landmark decisions such as Schrems II and the Microsoft Ireland case, will illustrate how courts navigate trans-border data issues.

The focus of this paper is limited to public and private regulatory frameworks that influence cross-border data governance. It will not address the technical aspects of data security or infrastructure but will concentrate on legal doctrines, regulatory instruments, and judicial reasoning. The structure of the paper is as follows: Section 2 outlines the theoretical and legal foundations of data sovereignty and data globalization; Section 3 discusses conflicting legal regimes; Section 4 analyses key case studies; Section 5 identifies core legal dilemmas; and Section 6 evaluates the potential for harmonization in international data governance. The conclusion synthesizes the findings and proposes possible legal pathways for the future.

II. THEORETICAL AND LEGAL FOUNDATIONS

A. Data Sovereignty

Data sovereignty is the principle asserting that data generated within a country's borders is governed by that nation's laws and regulatory frameworks. This concept extends the traditional Westphalian notion of sovereignty into the digital age, claiming jurisdiction over digital assets similarly to how physical territory is governed .

Data sovereignty is a term that underlines the nation’s control over the data that is processed and stored within the territory of a country, free from any kind of external influences. And the main aim of this is to secure data that I sensitive and personal.

The legal roots of data sovereignty are found in the constitutional law, administrative regulations, and specific data protection statutes. For instance, the European Union’s General Data Protection Regulation (GDPR) not only provides robust protections for personal data but also has extraterritorial applicability, meaning it governs data processing activities outside the EU if the data subject is located within the EU. Similarly, China’s Cyber security Law (2017) and Data Security Law (2021) establish state control over data deemed critical to national interests, enforcing localization requirements and allowing government access under certain conditions.

These laws show a growing trend where countries are taking back control over data by

treating it as part of their national authority. This means they may require data to be stored within their own borders, set rules on how different types of data are handled, and claim legal power over foreign companies that use their citizens' data. From a legal point of view, this idea of data sovereignty overlaps with international law and rules about which country's laws apply especially when data crosses borders and creates legal conflicts between countries.

Countries often say they need to control data to protect national security, keep public order, and defend their citizens' rights. But this kind of control can also cause problems. It might lead to digital protectionism (where countries block or limit foreign tech companies), break the global internet into separate pieces, and make it harder for different systems and countries to share data smoothly. As a result, when governments try to control data in the digital world, it creates tough questions about how much power they should really have and where that power should stop in a world where everything is connected online.

B. Data Globalisation

On the other hand, data globalization is about letting data move freely across countries, because that's essential for today's digital world to work properly. Things like cloud services, online shopping, social media, and international apps all depend on fast and smooth data sharing that doesn't stop at national borders.

From both legal and economic perspectives, data globalization is supported by international trade law, particularly through instruments like the World Trade Organization's General Agreement on Trade in Services (GATS) and newer digital trade provisions found in agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States, Mexico and Canada Agreement (USMCA). These international agreements usually try to reduce rules that force data to stay in one country and instead support data moving freely across borders. But they do make some exceptions for important public reasons, like safety or privacy. Big tech companies, like Google or Amazon, also help push global data sharing because they store and manage data in many different countries using cloud systems. These companies usually support laws that make it easier for data systems to work together and avoid too many restrictions, in line with ideas like keeping the internet open and fair for everyone.

But letting data flow freely around the world also brings some big legal problems. Different countries have different privacy laws and rules for protecting data, which can confuse both companies and users. On top of that, some countries, like those in the EU, apply their laws even outside their own borders, which make things even more complicated. There's also

growing concern about data colonialism where tech companies from rich countries collect data from people in poorer countries without giving them any real control or benefits in return. This has led to criticism of how global data is being handled today.

Thus, while data globalization fosters economic integration and innovation, it also reveals shortcomings in international legal frameworks and underscores the lack of a cohesive governance structure capable of balancing the competing interests of states, corporations, and individuals.

III. CONFLICTING LEGAL REGIMES

As countries create their own data regulations, significant differences in their laws are causing confusion and conflict, especially when data crosses borders.

A key example is the European Union's General Data Protection Regulation (GDPR). This law applies not only within the EU but also to companies outside the EU that collect or use data from EU citizens. This means that businesses in the U.S., India, or elsewhere must comply with the GDPR if they handle data from EU residents. While this enhances privacy protection, it creates legal tensions with countries that have different regulations.

In contrast, the United States uses a sectorial model, where various industries (like healthcare and finance) have their own privacy laws, but there is no comprehensive national data protection law. This fragmented approach makes it difficult to align with stricter regulations like the GDPR and results in gaps in privacy protections.

China has adopted a strict, sovereignty-focused approach with its Data Security Law and Personal Information Protection Law (PIPL). These laws give the government significant control over data, especially sensitive information, requiring companies to store certain data within China and obtain government approval before transferring it abroad.

India's recent Digital Personal Data Protection Act (2023) gives individuals more control over their personal data and allows the government to set rules on data storage. While it doesn't mandate full data localization like earlier proposals, it still grants the government considerable control, raising concerns about access and accountability.

These differing legal frameworks lead to major conflicts. For instance, a company operating in multiple countries may face conflicting rules on how to manage the same data. Questions about jurisdiction, such as which country's laws apply and who can enforce them are becoming increasingly complex. Additionally, when countries attempt to enforce their laws beyond their borders, it can lead to jurisdictional overreach, potentially causing diplomatic

 [ISSN 2581-5369]

tensions and complicating enforcement.

IV. CASE LAW ANALYSIS

To better understand how conflicts between national and global data laws play out in real life, it's important to look at some key court decisions and legal disputes. These cases highlight how difficult it is to balance national laws with the borderless nature of data.

A. The "Schrems" Cases – EU vs. US Data Transfers

The most well-known legal battles in this area come from the Schrems I and Schrems II cases. In Schrems I (2015), the European Court of Justice (ECJ) struck down the Safe Harbor Agreement, which allowed companies to move personal data from the EU to the US. The court said US law didn't give enough protection to EU citizens' data, especially against government surveillance.

In Schrems II (2020), the ECJ also invalidated the Privacy Shield agreement, which had replaced Safe Harbor. Once again, the court found that US surveillance laws conflicted with EU data protection standards. However, the court upheld the use of Standard Contractual Clauses (SCCs) a legal tool companies can use to transfer data internationally, so long as extra protections are added when needed.

These cases show how privacy rights in one country can block data transfers to another country, even if both are major trading partners. They also highlight the legal uncertainty businesses face when trying to comply with conflicting international rules.

B. Microsoft Ireland Case – Jurisdiction and Cross-Border Data Access

In United States v. Microsoft Corp. (2016), the US government tried to force Microsoft to hand over emails stored on a server in Ireland as part of a criminal investigation. Microsoft refused, arguing that US law didn't apply to data stored outside the country.

The case raised big questions about jurisdiction: does a country have the right to access data stored in another country, especially when it belongs to a foreign citizen? Before the Supreme Court could decide, the US passed the CLOUD Act (2018), which gave the government clearer powers to request data from US companies, even if the data is stored overseas.

This case showed how hard it is to balance law enforcement needs with data privacy and international law. It also highlighted the growing trend of extraterritorial legislation, where one country's laws try to reach beyond its borders.

 [ISSN 2581-5369]

C. Indian Case Law – Privacy and State Power

In Justice K.S. Puttaswamy v. Union of India (2017), the Indian Supreme Court declared that the right to privacy is a fundamental right under the Indian Constitution. This landmark judgment laid the foundation for India's Digital Personal Data Protection Act (2023), and it has been used to challenge excessive state surveillance and demand stronger data protection.

While the ruling pushed India toward a more privacy-focused legal system, it also left open questions about how far the state can go in collecting or accessing personal data, especially under laws that may allow government surveillance or data localisation.

V. BALANCING COMPETING INTERESTS

The challenge of regulating data across borders is not just a legal issue, it also involves balancing multiple, sometimes conflicting, interests. These include national security, economic growth, personal privacy, and international cooperation. Finding the right balance is difficult, and countries often prioritize these interests differently depending on their political systems, legal traditions, and levels of digital development.

A. Privacy vs. Commerce

At the heart of the data sovereignty vs. data globalization debate is the trade-off between privacy and commerce. Privacy advocates argue that people should have strong control over their personal data, and that governments should protect them from both corporate misuse and state surveillance. This is the view reflected in strict laws like the GDPR, which puts individual rights at the center of data regulation.

On the other hand, businesses- especially those in the tech sector, argue that too many restrictions on data make it harder to innovate, compete globally, and offer seamless digital services. Free-flowing data helps drive e-commerce, cloud computing, and artificial intelligence. This is why many trade agreements now include rules supporting cross-border data flows and limiting forced data localisation.

B. Sovereignty vs. Interoperability

Governments want to protect their sovereignty by making sure data about their citizens is handled according to their own laws and values. This is especially true in countries with strong national security priorities or concerns about foreign surveillance. However, this can create data silos, where each country's data is locked within its own borders, making global cooperation and system compatibility harder.

This becomes a real issue for companies and organizations trying to operate across multiple

countries. If each country has different rules, it's harder to make systems work together, a problem known as lack of interoperability. As a result, companies may have to build separate infrastructure for different regions, increasing costs and slowing down innovation.

C. Legal Certainty vs. Ethical Concerns

Legal frameworks like GDPR, China's PIPL, and India's new data law all try to provide legal certainty, clear rules that companies and users can rely on. But these laws also raise ethical concerns. For example, how much surveillance is too much? Can a government force companies to give them access to encrypted communications? Should companies profit from data collected in countries where people don't fully understand how their data is used?

These are not just legal questions but moral ones. There's growing concern that global data flows could reinforce digital inequality, where powerful countries and companies benefit from the data of users in weaker or poorer regions, without fair returns or protections.

VI. INTERNATIONAL EFFORTS AND FUTURE DIRECTIONS

As the conflicts between national data laws and global digital activity grow, international cooperation is becoming more important. Many countries and organizations are now trying to build shared rules for handling data across borders. However, progress is slow and often complicated by political differences, power imbalances, and competing national interests.

A. Global Governance Initiatives

Several efforts have been made to create international rules or frameworks for data governance:

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, revised 2013) were among the first global efforts to set standards for privacy and international data transfers. While not legally binding, they helped shape many national laws.

The G20 Osaka Track and Data Free Flow with Trust (DFFT) framework promoted by Japan aim to support free data flows while protecting privacy and security. However, these proposals are still vague and lack enforcement mechanisms.

The United Nations has also discussed data governance under broader debates about digital cooperation, but without strong legal outcomes so far.

Trade agreements like the CPTPP, USMCA, and EU–Japan Economic Partnership Agreement now often include specific chapters on digital trade and cross-border data transfers. These agreements aim to balance openness with regulatory rights, but they can also limit how far

countries can go in protecting their data sovereignty.

B. Regional Models and Soft Law Approaches

Because a single global treaty is unlikely in the near future, many regions are forming their own data governance models:

The European Union's GDPR has become a global benchmark, influencing laws in Brazil (LGPD), South Korea, India, and others. This is sometimes called the "Brussels Effect", when EU laws shape global practices even outside Europe.

In contrast, countries like China are building a "sovereignty-first" model, where data is treated as a national resource and subject to strong state control.

The APEC Cross-Border Privacy Rules (CBPR) system offers a voluntary, business-friendly model for privacy and cross-border data flows in the Asia-Pacific, but uptake remains limited.

Soft law like guidelines, codes of conduct, and international standards also plays an important role in shaping data practices across borders, especially when binding treaties are not possible.

C. Future Pathways

Looking ahead, the future of data governance will likely depend on a mix of legal harmonization, mutual recognition, and technology-based solutions. Some possibilities include:

Interoperable legal frameworks: Rather than forcing all countries to adopt identical laws, efforts may focus on making different legal systems work together through shared principles or mutual agreements.

Trusted data spaces: The EU's proposed European Data Spaces initiative imagines secure environments where data can be shared responsibly among trusted actors for research, innovation, or public services.

Tech-enabled accountability: Tools like data trusts, privacy-enhancing technologies (PETs), and blockchain-based auditing systems may help ensure that data is handled responsibly across borders, even when legal systems differ.

Still, all of these paths require on-going political will, trust between countries, and strong enforcement mechanisms out of which none are guaranteed.

 [ISSN 2581-5369]

VII. CONCLUSION AND RECOMMENDATIONS

A. Conclusion

This research explored the on-going legal challenges that arise from the tension between data sovereignty and data globalization. As digital technologies become more central to everyday life, the question of who controls data and under what rules, has become increasingly important. On one side, many countries want to keep tight control over data within their borders to protect national security, public order, and citizens' privacy. On the other side, the global digital economy depends on fast, free-flowing data that often moves across jurisdictions without clear boundaries.

The study showed that this legal clash creates serious issues in practice. International data transfers are frequently caught between different privacy laws, like the EU's GDPR and the U.S. sectoral approach, or between democratic and authoritarian models of data governance. High-profile cases like Schrems II and the Microsoft Ireland dispute highlight the confusion around jurisdiction and enforcement, especially when data is stored in one country but accessed or controlled from another.

Another key finding was that this legal uncertainty doesn't only affect companies but it also impacts ordinary users and raises ethical concerns. The concept of data colonialism is where powerful countries or corporations extract value from users in weaker regions shows that legal gaps can lead to deeper inequalities in the global data economy.

B. Recommendations

Based on the findings of this paper, several recommendations can be made:

1. **Work Toward Interoperable Legal Systems:** Instead of aiming for one global data law, countries should try to make their systems compatible. This means agreeing on core privacy principles while allowing for national differences. Mutual recognition agreements, like the EU's adequacy decisions, could be a helpful model.

2. **Encourage International and Regional Cooperation:** Global platforms like the G20, WTO, and OECD should be used to promote dialogue on data governance. At the same time, regional frameworks such as those developed by the EU, APEC, or African Union can create shared rules that reflect local values.

3. **Use Technology to Strengthen Trust**: New tools like privacy-enhancing technologies, data trusts, or secure multi-party computation can help reduce risks when data is shared across

borders. However, these tools should be supported by legal accountability and public transparency.

4. Protect Users in the Global South: There needs to be more focus on data justice. This means making sure users in developing countries are not just sources of raw data, but also have rights, protections, and a voice in global digital policy. This could involve creating stronger national data laws and pushing for fairer terms in international agreements.

5. Balance State Power and Personal Rights: Governments have a role in protecting data, but they must also respect individual rights. Surveillance powers should be limited by clear legal rules and independent oversight. At the same time, users should be empowered with more control over their personal information.

Final Thought

As this research has shown, the legal dilemmas around data sovereignty and globalization are complex, and there is no one-size-fits-all solution. However, with the right mix of legal reform, international cooperation, and ethical awareness, it is possible to build a global data system that supports both innovation and human rights.

The future of data governance will likely depend on how well we manage this balance. If states continue to tighten control over data without coordination, the risk is a fragmented internet, where information becomes trapped behind legal borders. This could harm not only businesses but also free expression, research collaboration, and social connectivity. On the other hand, a system that only promotes open data flows without adequate protections may expose individuals to exploitation, surveillance, and discrimination.

Therefore, a nuanced approach is needed where it acknowledges the legitimate interests of states, the economic importance of data flows, and the fundamental rights of individuals. As students and future legal professionals, understanding these dynamics is essential to shaping policies that are not only legally sound but also socially fair and globally relevant.

In the end, the debate over data sovereignty and globalization is not just about law or technology, it’s about the kind of digital world we want to live in, and who gets to decide its rules. This makes it one of the most pressing legal and ethical challenges of our time.

******

 [ISSN 2581-5369]

VIII. REFERENCES

1. Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press, 2020).
2. Burri, Mira. "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation." (2017) 51(1) UC Davis Law Review 65.
3. European Parliament and Council, Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L119/1.
4. Government of India, Digital Personal Data Protection Act, 2023.
5. G20, Osaka Leaders' Declaration, 28–29 June 2019.
6. Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance," (2021) 169 Privacy Laws & Business International Report 1.
7. Kuner, Christopher. Transborder Data Flows and Data Privacy Law (Oxford University Press, 2013).
8. Ministry of Industry and Information Technology (China), Data Security Law of the People's Republic of China (effective 1 September 2021).
9. Ministry of Industry and Information Technology (China), Personal Information Protection Law of the People's Republic of China (effective 1 November 2021).
10. OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013).
11. Parminder Jeet Singh, "Digital Industrialisation in Developing Countries: A Review of the Business and Policy Landscape" (IT for Change, 2020).
12. Schwartz, Paul M., and Daniel J. Solove. "Reconciling Personal Information in the United States and European Union." (2014) 102(4) California Law Review 877.
13. United States-Mexico-Canada Agreement (USMCA), Chapter 19: Digital Trade (2020).
14. World Trade Organization, WTO E-commerce Work Programme and Digital Trade Discussions, various reports (2018–2023).

*****

 [ISSN 2581-5369]