DATA SOVEREIGNTY VS. DATA PROTECTION: A COMPARATIVE CONSTITUTIONAL ANALYSIS OF INDIA'S PRIVACY LAWS AND GDPR

Ashutosh Panda, LLM, Lovely Professional University, Phagwara

Dr. Amit Kashyap, Associate Professor, Lovely Professional University, Phagwara

ABSTRACT

The current paradigms of data sovereignty and data protection discussed within this review of constitutional comparative analysis are domains influenced by the Digital Personal Data Protection Act 2023 (DPDPA) of India and the General Data Protection Regulation (GDPR) of the European Union. In India, Right to privacy has been declared as a fundamental right under Article 21 of the Constitution with the most notable Supreme Court decision being the justice K.S. Puttaswamy vs. Union of India. The driving force to a holistic law on privacy was the Union of India even though the DPDPA has moved this right by enforcing rules of processing of data that contain lawful processing, limitation of purpose, minimization of data, consent, transparency, and redress of grievances.

A key differentiating aspect of India's regime is the emphasis on data sovereignty. The DPDPA includes provisions for data localization, meaning that certain categories of data, such as payment or sensitive personal data, must be stored and processed within India's borders. However, selective trans-border data transfer to "trustworthy" jurisdictions is permitted. The emphasis of the DPDPA on data sovereignty aligns with national interests in economic control, law enforcement access, and national security. On the other hand, the principle of the GDPR is, in general, harmonized data protection regardless of where the data is located. The GDPR establishes free flow of data within the EU and freely to third countries as long as those countries have an adequate privacy legal regime.

Both legal regimes established robust user rights that included rights of accessing personal data, rights to correction of the personal data, and right of erasure albeit with different exceptions. GDPR limits government scoping over the rights related to national security to quite narrowly interpreted circumstances, whereas the DPDPA has broader exceptions based on public interest and sovereignty that would allow for governmental interference. Each legal including the DPDPA an GDPR include strict penalties,

respectively due to violation of those personal data protection regimes reflecting a shared commitment to privacy as a basic right.

Overall, this analysis show that while the India's Digital Personal Data Protection Act (DPDPA) is developed from the models of data protection established by the GDPR, it contemplates unique constitutional consideration along the same pathway of data sovereignty. The consideration of state interests, individual privacy, and data flows on a global scale motion the DPDPA along unique different pathways from the GDPR.

Keywords: Data Sovereignty, Data Protection, Digital Personal Data Protection Act (DPDPA), General Data Protection Regulation (GDPR), Fundamental Right to Privacy, Constitution of India Article 21, Data Localization.

INTRODUCTION

Data sovereignty and data protection now sit at the center of modern privacy law, especially as digital technologies erase borders and information moves across jurisdictions. Data sovereignty is about a nation's control and it states that data must follow the laws of the country where it is stored or created, often raising regulatory, political, and security questions. Data protection is about the individual and it safeguards personal information through rights, duties, and procedures, focusing on privacy regardless of where the data resides.

The connection between these concepts is very important in comparing legal systems. This can be seen in the ways India and the European Union approach these issues. India emphasizes data sovereignty by asserting national jurisdiction and control. Meanwhile, the EU's GDPR aims for consistent and strong data protection standards for individuals, applying even outside its borders when it comes to EU citizens' data. As countries try to find a balance between the flow of digital information and constitutional protections, understanding these basic concepts is essential for navigating current and future privacy laws.

Research Objectives

- To analyze and compare the constitutional foundations of data sovereignty and data protection in India and those of the European Union.
- To examine how India's DPDPA and the EU's GDPR define and put into practice the principles of data sovereignty and individual data protection.

- To assess how Article 21[1] of the Indian Constitution shapes privacy and data governance, and contrasts that constitutional approach with the GDPR's rights based architecture.

- To assess the impact and role of legal doctrines such as data localization, sovereignty, and cross-border data transfers on the privacy rights of individuals and state power in both the jurisdictions.

- To identify key comparisons and variations on compliance duties, enforcement mechanisms and user rights under the DPDPA and GDPR.

- To recommend practical policy and legislative approaches for harmonizing the twin goals of data sovereignty and data protection in a globally networked data ecosystem.

Research Questions

- How do India's Digital Personal Data Protection Act (DPDPA) and the EU's GDPR constitutionally define and reconcile the principles of data sovereignty and data protection?

- What constitutional and policy recommendations can be drawn for strengthening the synergy between data sovereignty and data protection in India?

- How does the legislative frameworks of India and the EU address data localization, cross-border data transfers, and jurisdictional challenges?

- What role does government discretion play in India's data protection rules vs. the EU's regulatory constraints?

RESEARCH METHODOLOGY

The research methodology for a comparative constitutional analysis of data sovereignty and data protection focuses upon India's privacy laws and the GDPR, typically involves a qualitative, doctrinal, and comparative approach as detailed below:

Qualitative Analysis: The study relies on primary legal sources by including the Indian

[1] The Constitution of India, art. 21.

Constitution, statutory laws like the DPDPA, 2023[2] of India and the GDPR[3] of the European Union. It also relies on policy instruments and landmark judicial decisions, especially the Puttaswamy judgment of the Supreme Court of India. The purpose is to investigate the application of data sovereignty and personal information protection principles in practice under the three distinct legal systems. The aim is to understand how the rules operate and are implemented in each jurisdiction, as well as identify the institutional choices and values that support them.

Comparative Framework: The study of comparing and contrasting the country's legal framework with the GDPR of EU and other international privacy regimes will be undertaken when it comes to cross border data flows and data localization. The objective is to examine how well these frameworks balance national interests with the global need for data governance and identify best practices that could be leveraged in the future.

Doctrinal Research: Legal principles, exceptions, rights, and government powers embedded in the laws to assess their alignment with constitutional values such as freedom of expression, privacy, national security, and sovereignty are the key areas of study.

Literature Review: From surveying academic articles, reports, and critiques to identifying gaps and debates in privacy law, data sovereignty, and digital governance.

Policy and Judicial Impact Assessment: Exploring the real-world consequences of these laws on individual rights, governmental authority, and international data governance, combined with reflections on compliance and enforcement mechanisms. This methodological mix enables a comprehensive understanding of the constitutional contours, legal intricacies, and policy implications surrounding data sovereignty and data protection in a globalized digital environment.

LITERATURE REVIEW

Digital Personal Data Protection Act (DPDPA), 2023 is a revolutionary legislation that recognizes data protection as a legal right and regulates the handling of personal data in India that includes, among others, processing, storage and transfer of personal data in India. The law

[2] *Digital Personal Data Protection Act, 2023.* MINISTRY OF ELECS. & INFO. TECH., GOV'T OF INDIA (Aug. 11, 2023),
[3] *The EU General Data Protection Regulation (GDPR)* 2018, (2016/679),

also establishes the Data Protection Authority for governance and also stipulates data localization and digital sovereignty for the protection of India's digital assets and citizens. Scholars identify data sovereignty as the state's territorial authority over in-country generated data and access to out-of-state stored data. India's data sovereignty efforts appear to follow the same trajectory as other nations that want to balance citizens' data privacy rights with national security, economic development, and autonomy goals. However, as per critics the requirements for data localization may hamper the free flow of information across borders and impede international digital trade by creating protectionist obstacles.

The GDPR model contrasts with India's regime by emphasizing the protection of data subjects' rights and free flow of personal data within and outside the EU based on adequacy determinations. The GDPR enforces respect to the law as one of the EU markets values and sets a benchmark for privacy regulations.

Current research highlights several significant difficulties with their implementation, such as potential government interference and the lack of clarity and independence concerning India's DPDPA draft rules. Judicial ruling such as India's Puttaswamy judgment, which enshrined privacy as a constitutional right is also significant.

The literature shows the dynamic interplay between data protection and data sovereignty with India and the EU charting unique but overlapping paths in pursuit of their constitutional, political, and economic imperatives thereby making this comparative constitutional analysis an important tool for understanding the future trajectory of global privacy governance.

RESEARCH & ANALYSIS

Constitutional Contextualization: Aims at analyzing provisions firmly established in the Indian constitution which stands within the fundamental rights, dimension to the Right to privacy supported by Article 21 of the Indian constitution. The EU Charter of Fundamental Rights, which serves as the basis for the GDPR is being regarded as more comprehensive in nature and this study attempts to decipher landmark judgments of the Honourable apex court of India in Puttaswamy v. Union of India with the Introduction of the European Union legal framework and proceeding to the establishments of the relevant data sovereignty and data protection indexes based on the legal system of the Union of India.

Legal Framework Comparison: To Look at the key features of Data Privacy Law in India known as Digital Personal Data Protection Act, 2023 (DPDPA) those of European Union called General Data Protection Rights (GDPR). Key focus areas are the data localization mandates, individual data rights, government exceptions, cross-border data transfer rules, enforcement mechanisms and penalty.

Data Sovereignty vs. Data Protection Tensions: Upon thorough examination it is found out how India tries to safeguard data sovereignty by enforcing data localisation and right of access to government personnel and agencies, while GDPR is built at the individual level and with protection and well-regulated data flow.

Impact Assessment: Appraises practical consequences of these laws on stakeholders, citizens, companies (comparatively fintech) and State Authorities. Studies compliance issues as well as enforcement experiences and judicial outcomes stated in relation to claims for data sovereignty and protection.

Policy and Judicial Developments: To monitor current regulatory changes and court decisions in both jurisdictions and identify areas where they are enhancing or breaking down the existing balance between sovereignty and privacy issues.

Synthesis and Recommendations: To Integrate the findings that suggest constitutional and policy reforms aiming to harmonize data sovereignty concerns with effective data protection and highlight lessons from GDPR implementation applicable to India's evolving framework.

Comparative Tensions and Shared Challenges

- **Comparative Tensions**

Data Sovereignty vs. Free Data Flow: The concept of data sovereignty highly determines data privacy debates in India. This translates to data localization needs and wide authorities of the government to get information. Instead, the European Union in the GDPR adheres to the example of promoting free cross-border data flow but only in the event that the country it goes to can offer satisfactory protections. This conflict highlights a conflict of priorities between Indian tendencies to national control and the EU approach to global digital interaction and seamless interaction.

The Right to State Control vs. the Right to the Individual: The legal system in India provides the state with a considerable amount of freedom, where data access can be provided due to national security and the interest of the people. Although they are important goals, they tend to threaten the privacy of individuals. Conversely, the GDPR considers data protection as one of the fundamental rights. It gives stringent restrictions to the state powers, which must be controlled by some form of oversight and judicial scrutiny, and thus puts the individual in the focus of data control. **Jurisdiction and Enforcement:** In its legislations on data privacy, India is largely territorial, as the GDPR is extraterritorial in nature. This implies that though India tends to regulate mostly within its geographical scope, GDPR is applicable to any company, regardless of the location in the globe, which handles the data of the EU citizens. Consequently, multinationals are forced to operate in two highly divergent compliance environments at the same time or both.

- **Shared Challenges**

Balancing Privacy with Security: India and the EU struggle to achieve the correct balance between the privacy of the individual and the legitimate state interests of national security, law enforcement, and protection of digital infrastructure. The difficulty is that security should not compromise the confidence of people in the greater data privacy system.

Complexity of regulatory compliance: In the case of businesses particularly multinational corporations, there is a complicated process of overcoming policy provisions. Regulations are not always clear in the two jurisdictions, which means that organisations are at a loss as to the compliance requirements whenever dealing with data that cuts across legal regimes.

Technological Evolution Outpacing Law: Legal systems are often outpaced by the pace of technological change especially in artificial intelligence, cloud computing, and other global digital platforms. This demands a continuous change in policy and judicial interpretation and both India and the EU are finding it difficult to future-proof their structures.

Data Governance and Institutional Capacity: Effective enforcement requires strong regulatory institutions. EU already possesses highly developed data protection authorities, and India is currently working on its institutional frameworks and enhancing them to reflect the self-sufficiency and checks and balances (similar to those in the GDPR frameworks).

International Cooperation Dilemmas:

Achieving global consistency in data protection law remains a daunting task as differing cultural, legal, and political approaches combined with geopolitical tensions and competing sovereignty claims by making mutual recognition of standards more difficult.

Significant Cases

India

- **Justice K.S. Puttaswamy (Retd.) vs. Union of India**[4]

  This landmark Judgement of the nine Judge bench of the Hon'ble Supreme Court of India was a confirmation of the Right to privacy as a fundamental right enunciated in the Art. 21 of the Indian constitution wherein it was unanimously decided that privacy is an essential feature of the right to life, liberty and freedom enshrined in the fundamental rights incorporated in the Chapter III of the Indian constitution. This decision reversed previous cases (Kharak Singh and M.P. Sharma) that have rejected privacy as a basic right. The Hon'ble Court held that, the Right to privacy may be restricted by the government only when there is compelling interest, and the restrictions must withstand tough legality, necessity, proportionality and thorough examination. The Court also held that any state's intrusion into personal privacy is acceptable only in compelling circumstances, and such exceptions will have to comply with principles of legality, necessity and proportionality especially in the context of the evolving data protection laws in India. This ruling was crucial considering developments on technology and data gathering, and created a constitutional ground on securing data and sovereignty in India. It also affected debates on Aadhaar system of biometric identification, individual and sexual rights, and broad privacy rights in relation to a state and non-state actors.

- **Shreya Singhal vs. Union of India**[5]

  The case involved the freedom of speech and expression as it relates to regulation of digital contents. It placed an emphasis on the equilibrium between personal rights and state sovereignty on the Internet. The information technology Act, 2000, section 66A was

[4] *Justice K.S. Puttaswamy (Retd.) vs. Union of India***,** AIR 2017 SC (CIV) 2714,
[5] *Shreya Singhal vs. Union of India,* AIR 2015 SC 1523,

considered in the case. This part criminalized the provision of offending or threatening messages using electronic equipment. The ambiguity of the words used in the legislation gave the authorities excessive authority to arbitrarily apply it and suppress legitimate expression. The decision of the court was that the provision was unconstitutional since it contravened Article 19(1) (a) of the Indian Constitution that provides the freedom of speech and expression. The court also highlighted that any restriction of the speech must be reasonable, well defined and should be in good faith and a lawful interest of the state and not overly broad or vague. The Supreme Court emphasized that free speech protection in online contexts is very crucial to democracy by striking down Section 66A. The case emphasized that, regulation of free speech on the internet should be formulated in a manner that does not broaden to censor dissent, satire, or criticism of a political or political organization. The case upheld that freedom of speech is necessary but it also stated that there should be fair boundaries that are reasonable and that should come after the constitutional protection against abuse. This ruling has played a crucial role in the legal debates on electronic rights over how an individual right against state interests can be established in controlling speech over the net.

European Union

- **Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)[6]**

- The court of justice of the EU dictated that people are entitled to be forgotten. This is one of the main points about personal control over personal information in accordance with the GDPR system. The Court ruled that search engines such as Google can be considered as data controllers since they receive, process, and present personal information in the search results. Thus, they have to adhere to the Data Protection Directive issued by EU (Directive 95/46/EC). This decision forced Google to pay attention to the EU data protection regulations despite it being a multinational enterprise. Notably, the ruling appreciated the right to be forgotten. People have the option of requesting search engines to delete what they consider to be old and irrelevant personal information. This is a compromise between the privacy rights against the rights of the people to access information. Nonetheless, this

[6] *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, CASE C-131/12, JUDGEMENT OF THE COURT (GRAND CHAMBER)MAY 13 2014, EU,.

right is not absolute and it has to balance out the interests of privacy of the individual and that of the populace.

- **Schrems II Case (Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems) (2020)[7]**

The Privacy Shield agreement was declared void by the CJEU with the emphasis on the rigid terms of cross-border data transfer. The case strengthened the need to balance between data sovereignty and data protection. Schrems II confirmed that the basic privacy rights took precedence over the EU law. It brought to the fore that the protection standards of international data transfers should be very high. It was stated in the case that wide-range solutions such as Privacy Shield cannot be sufficient without concrete protection. To be in compliance with the EU data protection laws companies should take certain steps. The case has transformed the global privacy practices where organizations have been advised to re-examine cross-border data flows and limit privacy rights to a globalized world.

- **Tele2 Sverige AB vs. Post- och telestyrelsen (2016)[8]**

The CJEU determined to restrict broad data retention imposed by states. The ruling focused on safeguarding against unwarranted government monitoring using the EU data protection principles. The Court determined that national laws that required retention of all data on traffic and location visited by all people without distinction infringed the Right to privacy and data protection as provided by the EU Charter. The Court emphasized that any privacy limitations should be focused, needed, and should be relatively in line with the legitimate end that they are aimed at achieving, such as combating serious crime. The decision further added that there should be checks by independent authorities in access to retained data, and this should uphold proportionality. The case has established a clear precedent that blanket data retention policies and free government access to the communication retained is not compatible with the EU fundamental rights.

CONCLUSION

[7] *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18, JUDGEMENT OF THE COURT (GRAND CHAMBER), JULY 16 2020, E.U,.

[8] *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State* for the Home Department v. Tom Watson and Others, JOINT CASES C-203/15 and C-698/15, 21 DEC 2016, (COJ EU).

Both the statutes seek similar goals, ensuring the protection of personal data while promoting accountability by data fiduciaries or processors, the frameworks of both laws implicitly differ given the priority of their respective jurisdictions.

The DPDPA of India evidences a high focus on data sovereignty, where data are required to be localized, and the government is granted a wide-ranging regulatory and enforcement authority. This emphasis reflects the national will to impose national jurisdiction upon personal data, to protect economic interests and to provide more security, which coincides with the constitutional framework putting privacy as one of the fundamental rights of the country but weighing it against the interests of the state as a whole.

On the other hand, GDPR focuses on the basic right to a data protection in the context of a harmonized, extra-territorial environment. It supports the free movement of data inside and outside the EU that is organized on the basis of rigid provisions of individual rights, transparency, and accountability that aim at empowering individuals and limiting the governmental overreach.

Although the two regimes have common aspects of ensuring personal data protection, their differences in the perception of sovereignty and cross-border regulation brings conflicts especially in relation to international data transmission and international regulations as a source of regulatory compliance to global business. The same issues are still unresolved in terms of privacy and security demands, technological change at a faster rate than legislation, and effective implementation.

Finally, a novel data protection framework in India, inspired by yet distinct to the GDPR, is indicative of a calculated effort to balance the constitutional (and sovereignty) imperatives with the increased demands of individual privacy protection in a digital worldwide environment. This comparison and contrast suggests the need to further the policy discussion and legal refinement of these two objectives to put the interconnected world into balance.

As the study suggests, the future of privacy regulation is to design frameworks that would enhance national sovereignty and encourage the enhancement of the national protection of personal data, the development of trust, innovations, and collaboration across borders in the digital era.

BIBILOGRAPHY

- India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison by Latham & Watkins LLP.
- Data Protection Frameworks of India and the US by Institute for Defence Studies and Analyses (IDSA), March 2025.
- India's Digital Personal Data Protection Act 2023 vs. the GDPR, Global Privacy Blog, January 2024.
- Data Protection and Data Privacy, Comptroller and Auditor General of India, 2024.
- Cross-Border Data Flows and India's Digital Sovereignty, Verfassungsblog, March 2025.
- Comparative Overview of Global Data Sovereignty, Cloud Security Alliance, January 2025.
- Understanding India's New Data Protection Law, Carnegie Endowment for International Peace, October 2023.
- India's Digital Dilemma: Between Global Integration and Data Protection - ISPI, 2025.
- Data Sovereignty: Challenges and Considerations - Cloudian, November 2023.
- Data Sovereignty and Data Residency: A Comparison - IBM, January 2025.
- Data Protection Laws in India - DLA Piper, April 2024.
- Data Sovereignty and Data Protection in the Digital Economy - Stackscale Blog.
- ILI Law Review Summer Issue 2021: Data Sovereignty - Indian Law Institute.