International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Sovereignty Vs Privacy: Navigating The Digital Divide

[1]Mahima Sharma & [2]Dr. Sanskriti Srivastava

[1]Ph.D. Research Scholar & [2]Assistant Professor

Department of Law

Apex University, Jaipur

Abstract

In the digital age, the tension between national sovereignty and individual privacy rights has emerged as one of the most pressing legal and ethical challenges facing governments, corporations, and citizens worldwide. As data transcends geographical boundaries with unprecedented ease, nations assert control over digital infrastructure and information flows to protect their sovereignty, security, and economic interests. Simultaneously, international frameworks like the General Data Protection Regulation (GDPR) and laws such as the U.S. CLOUD Act reflect divergent approaches to balancing state authority with privacy rights. This article examines the fundamental conflict between data sovereignty and individual privacy, exploring how different jurisdictions navigate this complex landscape through regulatory frameworks, legal precedents, and enforcement mechanisms. By analyzing key legislations including India's Digital Personal Data Protection Act 2023, the EU's GDPR, and the U.S. CLOUD Act, this article illuminates the challenges of harmonizing global data governance while respecting both sovereign prerogatives and fundamental privacy rights.

Introduction

Data has become both currency and weapon in contemporary global affairs, positioning the concept of digital sovereignty at the heart of a profound dilemma (Frosinini, 2025). Nations increasingly assert control over data flows, digital infrastructure, and technological ecosystems to protect citizens' privacy, ensure security, and reclaim autonomy from foreign technological dominance. However, this wave of digital nationalism risks fragmenting the open internet, disrupting cross-border trade, and complicating the information exchange that underpins modern economies.

The intersection of sovereignty and privacy raises significant legal and ethical questions regarding the balance of power and individual liberties (World Jurisprudence, 2024). While states exercise sovereign rights by implementing laws affecting citizens' privacy often justified by national security concerns and public order-these measures can compromise fundamental privacy rights. Conversely, privacy rights can serve as a check on state sovereignty, allowing citizens to challenge governmental overreach. This complex relationship necessitates careful legal examination of how different jurisdictions balance state authority with individual rights in an increasingly interconnected world.

Understanding Data Sovereignty

Data sovereignty refers to the principle that data is subject to the laws and regulations of the country where it is collected, processed, and stored (Wire, 2025). It means an organization's right to control and regulate data generated and owned by the organization, ensuring that data

is protected and kept within jurisdictional boundaries (Thales, 2025). This concept has evolved from being ostracized to becoming central to current digital policy-making (Diplomacy.edu, 2025).

Data sovereignty goes beyond mere geography—it encompasses privacy, control, and trust in the digital ecosystem (Consultancy.eu, 2026). The emphasis extends to preventing loss of exclusive control over sensitive data, avoiding legal conflicts where complying with foreign requests may violate domestic privacy rights, and mitigating reputational risks particularly in sectors with high privacy expectations such as healthcare, public sector, and finance.

Privacy As A Fundamental Right

The right to privacy encompasses an individual's entitlement to personal autonomy and protection from unwarranted intrusion by both the state and private entities (World Jurisprudence, 2024). In India, the right to privacy has been declared a fundamental right under Article 21 of the Constitution, with the landmark Supreme Court decision by Justice K.S. Puttaswamy establishing this principle (IJLLR, 2025). Similarly, the European Union's GDPR establishes personal data protection as a fundamental right with extraterritorial applicability (N-IX, 2025).

Privacy rights create a critical check on state sovereignty. Core principles underpinning this balance include proportionality, which mandates that restrictions on individual rights must be appropriate and not excessively burdensome relative to intended public interest, and due process, which requires transparent procedures safeguarding fundamental liberties (Sphere of Law, 2024). However, governments increasingly use digital surveillance to enhance security, raising questions about the extent to which due process safeguards protect privacy in the digital age.

The Regulatory Landscape

European Union: GDPR Framework

The EU's GDPR establishes personal data protection as a fundamental right and extends its reach beyond Europe's borders through extraterritorial applicability (N-IX, 2025). The regulation obliges organizations to maintain lawful processing, minimize collection, provide individual rights such as access and erasure, and restrict cross-border transfers unless the destination country ensures adequate protection. The Schrems II judgment further tightened these rules by invalidating Privacy Shield and demanding supplementary safeguards even where Standard Contractual Clauses are used.

GDPR makes sovereignty less about physical storage and more about legal authority: European data must remain governed by EU law, wherever it resides (N-IX, 2025). The EU Data Act, becoming applicable on September 12, 2025, redefines sovereignty by addressing non-personal and industrial data, introducing rights for users to access and port data generated by connected devices and preventing vendor lock-in practices. It prohibits unlawful third-country access to non-personal data stored or processed in the EU, underscoring that sovereignty extends beyond personal information to cover industrial, IoT, and operational datasets.

India: Digital Personal Data Protection Act 2023

India's Digital Personal Data Protection Act 2023 (DPDPA) reflects a sovereignty-centric philosophy that prioritizes national control over data governance (IJLLR, 2025). A key differentiating aspect is the emphasis on data localization, meaning 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 (InCountry, 2024).

The DPDPA empowers the central government to restrict data transfers to countries lacking adequate protections, a clear assertion of sovereign prerogative under the guise of protecting informational autonomy (IJALR, 2025). The Indian government retains authority to regulate and restrict data transfers in cases of national security, public order, or sovereignty concerns. While the Act empowers individuals with rights to access, correct, and delete data, it includes broader exceptions based on public interest and sovereignty that allow for governmental interference, contrasting with GDPR's narrowly interpreted national security exceptions.

United States: CLOUD Act

The U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act represents a fundamentally different approach, prioritizing law enforcement access to data over individual control (AI-Legal Insight, 2025). The Act explicitly states that stored data sought under the Stored Communications Act must be disclosed regardless of where the data is physically located, as long as the provider is subject to U.S. jurisdiction. This territorial approach directly challenges traditional notions of data sovereignty.

From a privacy perspective, the CLOUD Act prioritizes law enforcement access whereas regimes like GDPR prioritize individual control over personal data (AI-Legal Insight, 2025). This fundamental difference has led to concerns that the Act may undermine privacy guarantees, especially for foreigners whose data may be accessed by U.S. agencies. Non-U.S. individuals are particularly vulnerable: their data can be accessed by U.S. agencies under a legal regime where they have no direct voice. The Act does require that partner nations uphold basic human rights and that an independent authority review orders, with agreements including numerous provisions protecting privacy and civil liberties (Osler, 2025).

The Fundamental Conflict

The evolving global data privacy landscape reflects a deeper dialectic between cosmopolitan legalism and nationalistic legal pluralism (IJALR, 2025). As data increasingly traverses borders seamlessly, states assert regulatory control to protect citizens while simultaneously participating in global digital commerce. This creates several critical tensions that manifest across multiple dimensions.

Legal Conflicts and Jurisdictional Challenges

Legal conflicts emerge where complying with one jurisdiction's request may violate another's privacy rights, EU data protection, or confidentiality obligations (Consultancy.eu, 2026). The case of transatlantic data flows exemplifies this tension—the framework has been repeatedly invalidated by European courts, with each attempt to patch the regime through new agreements facing legal challenges. The latest Transatlantic Data Privacy Framework created in 2023

introduces a Data Protection Review Court and new certification mechanisms, yet critics argue it replicates previous flaws by relying on executive orders rather than statutory reforms (Frosinini, 2025).

National Security Versus Individual Privacy

National security justifications for restricting data flows can mask mass surveillance concerns (Frosinini, 2025). When governments enforce data localization, they may gain easier access to citizens' data. Conversely, unrestricted data flows can allow foreign intelligence agencies or corporations to exploit personal information. The U.S. Protecting Americans from Foreign Adversary Controlled Applications Act targets apps like TikTok, aiming to prevent exploitation of user data by foreign governments, yet critics argue such policies could lead to balkanization of the internet and provide cover for domestic surveillance.

The potential for overreach poses significant concerns within the framework of due process (Sphere of Law, 2024). When state power is exercised without adequate checks, it can lead to infringement of fundamental rights such as privacy, free expression, and due process itself. Broad surveillance laws, purportedly for national security, can violate privacy rights if not properly limited or scrutinized, eroding trust in the legal system and perpetuating abuses of power.

Economic and Compliance Challenges

For multinational businesses, navigating conflicting sovereignty and privacy regimes creates substantial compliance burdens and strategic challenges. Organizations face increased scrutiny from regulators and customers, particularly in sectors with high privacy expectations (Consultancy.eu, 2026). Regulators are increasingly auditing and penalizing companies who mismanage cross-border data, with enforcement actions becoming more frequent in 2025 (Exasol, 2025).

Trade agreements prioritize economic efficiency and market access over human rights, creating structural bias that makes them ill-suited to guarantee robust privacy protections (Frosinini, 2025). Traditional trade law was designed to lower tariffs and harmonize standards for goods, never meant to address fundamental rights like privacy. This creates tension between privacy, security, and economic interests, with the U.S. withdrawal from certain digital trade provisions highlighting these competing priorities.

Emerging Trends and Future Directions

As 2025 progresses, several trends are reshaping the sovereignty-privacy landscape (Exasol, 2025). Regulators are conducting more enforcement actions with increased penalties for non-compliance. Compliance automation tools are becoming more sophisticated and embedded as a core business function. Greater customer scrutiny is emerging, with consumers reading privacy policies and asking harder questions about data handling practices.

The NIS2 Directive, transposed by Member States in October 2024 and entering enforcement through 2025, extends cybersecurity obligations across broader sectors, reinforcing the link between data sovereignty and security (N-IX, 2025). Cloud sovereignty remains firmly on the European agenda, with organizations seeking solutions that provide control and trust without compromising innovation or global connectivity.

Towards a Balanced Framework

A balanced framework must reconcile sovereign prerogatives of individual states with demands of interoperable privacy governance (IJALR, 2025). This necessitates institutionalization of normative dialogues through mechanisms such as adequacy decisions, bilateral data transfer frameworks, and multilateral conventions on data protection. Both the EU and India must cultivate judicial environments responsive to the nuances of digital sovereignty while maintaining robust privacy protections.

The challenge lies in balancing legitimate pursuit of sovereignty with the collaborative spirit required for global digital interdependence (Frosinini, 2025). Striking this balance requires legal safeguards to prevent overreach without compromising necessary security measures, ensuring due process remains integral to privacy protections while respecting each nation's right to govern its digital landscape.

Conclusion

The tension between sovereignty and privacy represents one of the defining challenges of the digital age. While sovereignty empowers nations to protect their citizens, infrastructure, and economic interests, privacy safeguards fundamental human rights and individual autonomy. Neither principle can be sacrificed entirely without profound consequences for democratic governance, international commerce, and human dignity.

The divergent approaches embodied in GDPR's rights-based framework, India's sovereignty-centric model, and the U.S. CLOUD Act's law enforcement priorities illustrate the complexity of achieving harmonization in global data governance. As digital technologies continue to evolve and data flows intensify, the international community must develop flexible yet principled frameworks that respect both sovereign authority and individual rights. Only through sustained dialogue, mutual recognition of legitimate interests, and commitment to fundamental human rights can the global community navigate the digital divide between sovereignty and privacy.

References

1. AI-Legal Insight. (2025, July 23). The U.S. CLOUD Act: Balancing cross-border data access, privacy, and sovereignty. https://ai-legalinsight.com/34-the-u-s-cloud-act-balancing-cross-border-data-access-privacy-and-sovereignty/
2. Consultancy.eu. (2026, February 9). Data sovereignty goes beyond geography – it's about privacy, control and trust. https://www.consultancy.eu/news/13168/data-sovereignty-goes-beyond-geography-its-about-privacy-control-and-trust
3. Diplomacy.edu. (2025, April 28). Digital sovereignty: The end of the open internet as we know it? (Part 1). https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/
4. Exasol. (2025, July 22). Data sovereignty trends: What businesses need to know in 2025. https://www.exasol.com/blog/data-sovereignty-trends/
5. Frosinini, A. (2025, October 17). Digital sovereignty dilemma: Balancing privacy, power and trade in a fragmented world. LinkedIn. https://www.linkedin.com/pulse/digital-sovereignty-dilemma-balancing-privacy-power-trade-frosinini-ajxlf

6. InCountry. (2024, December 1). Comprehensive guide to Indian data privacy laws. https://incountry.com/blog/comprehensive-guide-to-indian-data-privacy-laws/
7. International Journal of Advanced Legal Research. (2025, May). The clash between sovereignty and privacy: A need for regulatory compliance shaping the global data landscape. IJALR, 5(4). https://ijalr.in/
8. International Journal of Law and Legal Research. (2025, September 29). Data sovereignty vs. data protection: A comparative constitutional analysis of India's privacy laws. https://www.ijllr.com/post/data-sovereignty-vs-data-protection-a-comparative-constitutional-analysis-of-india-s-privacy-laws
9. N-IX. (2025, September 23). Data sovereignty: In-depth guide for compliance & resilience. https://www.n-ix.com/data-sovereignty/
10. Osler. (2025, November 25). Data sovereignty in light of the CLOUD Act: Back to the future. https://www.osler.com/en/insights/updates/data-sovereignty-in-light-of-the-cloud-act-back-to-the-future/
11. Sphere of Law. (2024, June 30). Navigating the balance between state interests and individual rights in law. https://sphereoflaw.com/balancing-state-interests-and-individual-rights/
12. Thales. (2025, June 9). Why data sovereignty and privacy matter. https://cpl.thalesgroup.com/blog/encryption/data-sovereignty-privacy-governance
13. Wire. (2025, October 6). Digital sovereignty in 2025: Why it matters for European enterprises. https://wire.com/en/blog/digital-sovereignty-2025-europe-enterprises
14. World Jurisprudence. (2024, June 13). Sovereignty and the right to privacy: A global perspective. https://worldjurisprudence.com/sovereignty-and-the-right-to-privacy/