CROSSING BORDERS: COMPARATIVE PERSPECTIVES ON DATA PROTECTION LAWS IN INDIA, THE EU, AND THE US

Vaibhav Yadav*

ABSTRACT

In an era where digital data transcends territorial boundaries, the imperative to establish robust and harmonized data protection regimes has gained unprecedented significance. This research article, titled "Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU, and the US", critically examines the evolution, scope, and effectiveness of data protection frameworks in three key jurisdictions. The European Union's General Data Protection Regulation (GDPR) is often hailed as the gold standard for data privacy, with its rights-based approach and stringent compliance mechanisms. In contrast, the United States adopts a sectoral and market-driven model, where privacy regulation varies by industry and is deeply influenced by commercial interests. India, poised at a regulatory crossroads, is in the process of enacting the Digital Personal Data Protection Act, 2023, which reflects a hybrid model influenced by both EU and US systems, yet tailored to its constitutional and socio-economic context. The article undertakes a comparative legal analysis to identify strengths, gaps, and convergence points among these regimes, especially in relation to consent, data localization, enforcement, and individual rights. It further interrogates how these differences impact global data governance, cross-border data flows, and the protection of fundamental rights in a digitized world. By highlighting the challenges of legal interoperability and proposing pathways for regulatory coherence, the study contributes to the ongoing discourse on data sovereignty, privacy ethics, and the future of digital governance.

KEYWORDS: Data Protection, Privacy Law, Cross-Border Data Flow, GDPR, Digital Personal Data Protection Act, Data Governance.

* Teaching and Research Associate, Gujarat National Law University, Gandhinagar, India

INTRODUCTION

In an increasingly digitised world, personal data has become one of the most valuable commodities. As individuals interact more frequently with digital platforms, vast amounts of data are generated, stored, and processed; often without a clear understanding of how such data is used or transferred. The rise of big data analytics, artificial intelligence, and global cloud infrastructure has intensified the need for comprehensive and robust legal frameworks to protect individuals' privacy rights. In this context, data protection laws are not merely regulatory instruments but essential legal safeguards to uphold the dignity, autonomy, and informational self-determination of individuals.[247] This paper undertakes a comparative legal analysis of data protection regimes in India, the European Union (EU), and the United States (US), three jurisdictions that represent distinct normative, legal, and institutional approaches to data privacy.

The significance of studying data protection laws through a comparative lens lies in the transnational nature of data flows and the global operations of digital platforms. With increasing instances of data breaches, algorithmic profiling, and cross-border surveillance, data protection is no longer a domestic issue. Rather, it is situated at the intersection of human rights, commercial interests, and state security.[248] The European Union, through the General Data Protection Regulation (GDPR), has adopted a rights-based, comprehensive regulatory framework that has set a global benchmark for privacy governance.[249] The United States, on the other hand, follows a sectoral and market-oriented approach, characterised by fragmented federal and state-level legislations.[250] India is currently navigating the complexities of crafting a comprehensive privacy law through the Digital Personal Data Protection Act, 2023 (DPDP Act), which seeks to harmonise individual rights with state and economic imperatives.[251] These three jurisdictions thus offer varied yet interconnected paradigms of privacy regulation.

OBJECTIVES, RESEARCH QUESTIONS AND METHODOLOGY

The objective of this research is to examine and compare the conceptual foundations, legislative instruments, and institutional mechanisms of data protection laws in India, the EU, and the US. It seeks to identify points of convergence and divergence in their treatment of key principles such as consent, data minimisation, purpose limitation, and enforcement.

---

[247] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015)
[248] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019)
[249] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)
[250] California Consumer Privacy Act 2018, Cal Civ Code §§ 1798.100–1798.199
[251] Digital Personal Data Protection Act 2023 (India)

Furthermore, it explores how each legal system balances the competing interests of privacy, innovation, and national security, particularly in relation to cross-border data transfers and surveillance practices. The analysis also aims to evaluate the emerging global trends in data governance and the possibility of achieving regulatory interoperability among different legal regimes.[252]

The central research questions guiding this study are: How do India, the EU, and the US differ in their legal treatment of personal data protection? What are the normative and practical implications of these differences for individuals and digital service providers? Can a global framework for data protection be envisioned that respects jurisdictional sovereignty while ensuring a minimum standard of privacy rights across borders?

Methodologically, the research adopts a comparative doctrinal approach. It draws upon primary legal instruments such as statutes, regulations, constitutional provisions, and judicial decisions from the three jurisdictions. Secondary sources including scholarly articles, government reports, and expert commentary are also consulted to provide a nuanced understanding of the evolution and implementation of data protection laws. The focus is primarily on substantive legal analysis, while also engaging with the broader political and economic contexts that shape data governance in each region.[253]

The scope of this paper is limited to the legal frameworks governing the protection of personal data in India, the EU, and the US. While it touches upon international instruments and principles; such as those developed by the OECD or under the UN; it does not offer a detailed analysis of multilateral treaties or regional agreements beyond the three focal jurisdictions. The paper also does not provide an exhaustive treatment of cybersecurity laws, though it recognises the overlap and interaction between data protection and information security regulations.

This chapter sets the stage for the subsequent analysis by framing data protection as a multidimensional legal issue with global implications. The next chapter provides an in-depth overview of the data protection regimes in the EU, US, and India, tracing their historical development, key features, and regulatory philosophies. The aim is to build a foundational understanding before undertaking a detailed comparative evaluation.

The growing prominence of data privacy in legal and policy discourses underscores the need for harmonised regulatory responses that can withstand the pressures of technological innovation and geopolitical contestation. While absolute uniformity may be neither possible

[252] Graham Greenleaf, 'Global Data Privacy Laws 2023: Despite Challenges, 162 Laws Show GDPR Dominance' (2023) 181 *Privacy Laws & Business International Report* 1

[253] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD 2013)

nor desirable, recognising the shared principles and distinctive approaches of different legal systems is essential for crafting more inclusive and effective data protection norms. As nations navigate the complex terrain of digital governance, the comparative perspective offered in this study is not only timely but necessary for understanding the legal architecture of privacy in a globalised world.[254]

DATA PROTECTION FRAMEWORKS: AN OVERVIEW OF INDIA, THE EU, AND THE US

EVOLUTION AND LEGISLATIVE FRAMEWORKS

The evolution of data protection laws across India, the European Union (EU), and the United States (US) reflects a diverse range of normative commitments, institutional traditions, and socio-political imperatives. While all three jurisdictions acknowledge the need to regulate the collection and processing of personal data, their legal approaches vary significantly in both scope and depth. The European Union has been at the forefront of privacy and data protection legislation. Its efforts began with the Data Protection Directive of 1995, which was later replaced by the General Data Protection Regulation (GDPR) in 2016, fully enforceable from May 2018.[255] The GDPR adopts a rights-based and harmonised framework that is directly applicable in all member states. It enshrines key principles such as transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.[256] Most notably, the GDPR recognises the right to data protection as a fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union.[257]

In contrast, the US follows a sectoral approach to data protection, lacking a comprehensive federal law. Instead, it has enacted a range of federal statutes focused on specific types of data or industries, such as the Health Insurance Portability and Accountability Act (HIPAA) for health data, the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA) for financial data.[258] The California Consumer Privacy Act (CCPA), and more recently the California Privacy Rights Act (CPRA), mark a significant shift toward a more EU-style privacy framework at the state level, introducing rights such as access, deletion,

[254] Justice K S Puttaswamy v Union of India (2017) 10 SCC 1
[255] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995
[256] Regulation (EU) 2016/679 (General Data Protection Regulation), art 5
[257] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8
[258] Health Insurance Portability and Accountability Act of 1996, Pub L No 104–191; Children's Online Privacy Protection Act of 1998, 15 USC §§ 6501–6506

and opt-out of data sales.[259] However, these state laws still fall short of the comprehensive protections offered by the GDPR.

India's journey towards data protection legislation has been shaped significantly by judicial intervention and policy discourse. In the landmark case of *Justice K. S. Puttaswamy v Union of India* (2017), the Supreme Court of India declared the right to privacy as a fundamental right under Article 21 of the Constitution.[260] This judicial pronouncement paved the way for legislative action, culminating in the enactment of the *Digital Personal Data Protection Act, 2023 (DPDP Act)*. The DPDP Act outlines the obligations of data fiduciaries, recognises the rights of data principals, and proposes the establishment of the Data Protection Board of India. It emphasises consent-based processing, data minimisation, and purpose limitation, reflecting global best practices.[261]

KEY FEATURES AND INSTITUTIONAL MECHANISMS

Each jurisdiction has developed institutional and regulatory mechanisms tailored to its legal framework. In the EU, data protection authorities (DPAs) are established in each member state to monitor compliance with the GDPR. The *European Data Protection Board (EDPB)* serves as a central body to ensure consistent application and resolve cross-border disputes.[262] The GDPR grants DPAs significant enforcement powers, including the authority to impose fines up to €20 million or 4% of a company's global annual turnover, whichever is higher.[263]

In the US, institutional regulation is fragmented. Different agencies, such as the *Federal Trade Commission (FTC)* and *Department of Health and Human Services (HHS)*, oversee compliance within their respective domains. The FTC, in particular, plays a pivotal role in consumer protection, often using its authority under Section 5 of the FTC Act to address unfair or deceptive practices in the realm of privacy.[264] However, the lack of a dedicated federal data protection authority limits the scope and coherence of enforcement.

India's DPDP Act proposes the formation of a central *Data Protection Board of India*, empowered to handle grievances, impose penalties, and ensure compliance. While the Act aligns with many principles found in the GDPR, it differs in some aspects, such as its approach to deemed consent and the broad exemptions provided to the state for reasons of national

[259] California Consumer Privacy Act 2018, Cal Civ Code §§ 1798.100–1798.199; California Privacy Rights Act 2020
[260] Justice K S Puttaswamy v Union of India (2017) 10 SCC 1
[261] Digital Personal Data Protection Act 2023 (India)
[262] Regulation (EU) 2016/679, arts 51–70
[263] ibid, art 83
[264] Federal Trade Commission Act 1914, 15 USC § 45

security or public interest.[265] The Indian framework also places significant emphasis on localisation, mandating that critical personal data be stored within the country—a feature absent in both the EU and US models.[266]

Cross-border data transfers are another area where differences become stark. The GDPR permits such transfers only to countries that ensure an adequate level of data protection or under appropriate safeguards like Standard Contractual Clauses (SCCs). The US, until recently, operated under the Privacy Shield Framework, which was invalidated by the Court of Justice of the EU in the *Schrems II* decision for failing to ensure adequate protection against government surveillance.[267] India's approach remains in flux, with policy debates ongoing regarding localisation requirements and strategic data partnerships.

Despite the varying models, common principles—such as accountability, transparency, and the importance of informed consent—form the backbone of data protection regimes in all three jurisdictions. However, the degree of enforceability, the role of individuals, and the independence of regulatory authorities diverge sharply. The EU's rights-based model places the individual at the centre, while the US framework focuses on consumer choice and market regulation. India's model, meanwhile, attempts to balance individual rights with state interests and economic development.

In summary, this chapter has laid the foundation for a deeper comparative analysis by highlighting the historical, legislative, and institutional contours of data protection laws in India, the EU, and the US. The next chapter will examine specific principles such as consent, data subject rights, enforcement mechanisms, and cross-border data transfer regimes in greater detail to map the points of convergence and divergence across these three legal systems.

COMPARATIVE ANALYSIS OF KEY PRINCIPLES IN DATA PROTECTION

CONSENT, DATA SUBJECT RIGHTS, AND PURPOSE LIMITATION

A comparative study of the data protection frameworks in India, the EU, and the US reveals both convergence and divergence in foundational legal principles. Among these, the principles of consent, data subject rights, and purpose limitation are central to regulating the relationship between individuals and entities processing personal data.

Consent serves as a foundational ground for lawful data processing in both the EU and India. Under Article 6 of the GDPR, consent must be "freely given, specific, informed and

[265] DPDP Act 2023, s 17
[266] Government of India, *Draft National e-Commerce Policy* (2019)
[267] Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems [2020] ECLI:EU:C:2020:559

unambiguous," and requires an affirmative act by the data subject Furthermore, Article 7 of the GDPR stipulates that data subjects must have the right to withdraw.[268] consent at any time, making it a dynamic and ongoing process. In India, the *Digital Personal Data Protection Act, 2023 (DPDP Act)* also mandates that data fiduciaries obtain clear and affirmative consent, which must be accompanied by a notice explaining the purpose of processing.[269] However, the DPDP Act introduces the concept of "deemed consent" in certain situations—such as when personal data is voluntarily provided by the user—which dilutes the stringency of consent requirements when compared to the GDPR.[270]

In contrast, the US approach is largely sectoral and contractual. Consent often takes the form of privacy policies or terms and conditions which users accept—usually without reading them; before accessing a service. While this satisfies legal requirements under laws like COPPA or HIPAA, it often falls short of the standard of "informed consent" established in the EU model.[271] Moreover, "opt-out" models, which place the burden on users to deny permission, are prevalent in US frameworks, unlike the EU's preferred "opt-in" standard.

Data subject rights are robustly articulated in the GDPR. These include the right to access, rectify, erase (the "right to be forgotten"), restrict processing, object to processing, and the right to data portability.[272] These rights empower individuals to exercise control over their personal data and challenge any misuse. The DPDP Act mirrors several of these rights, notably the rights to access, correct, and erase personal data. However, the effectiveness of these rights in India is yet to be tested, especially given the broad exemptions provided to the state in matters of national interest.[273]

In the US, the articulation of data subject rights is fragmented and inconsistent across sectors. The CCPA and CPRA provide Californian residents with rights similar to the GDPR, such as the right to access and delete personal data, and the right to opt-out of the sale of their data. However, these rights are not available uniformly across all states or sectors, leading to a patchwork of protections that are often confusing for both users and businesses.[274]

Purpose limitation, another core principle, requires that data collected must be used only for the specific purposes stated at the time of collection. The GDPR strictly enforces this through

---

[268] Regulation (EU) 2016/679 (General Data Protection Regulation), arts 6–7
[269] Digital Personal Data Protection Act 2023 (India), s 5
[270] ibid, s 7
[271] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in J Lane and others (eds), *Privacy, Big Data, and the Public Good* (CUP 2014)
[272] GDPR, arts 15–20
[273] DPDP Act 2023, s 17
[274] California Consumer Privacy Act 2018, Cal Civ Code §§ 1798.100–1798.199; California Privacy Rights Act 2020

Article 5, ensuring that any further processing must be compatible with the original purpose.[275] The DPDP Act incorporates a similar principle but allows for broader exceptions, especially where consent deemed is invoked. In the US, the idea of purpose limitation is generally embedded in individual statutes (e.g., health data must be used for medical purposes), but there is no overarching principle applicable across all types of data.

ENFORCEMENT, REMEDIES AND CROSS-BORDER DATA TRANSFERS

The enforcement mechanisms in each jurisdiction reflect the philosophical underpinnings of their data protection regimes. In the EU, the *Data Protection Authorities (DPAs)* have far-reaching powers, including the ability to conduct audits, issue warnings, and impose administrative fines. The landmark *€746 million fine imposed on Amazon by Luxembourg's DPA* in 2021 demonstrates the EU's commitment to enforcement[9]. Furthermore, individuals have direct access to judicial remedies and can file complaints with DPAs or courts in case of violations.

India's DPDP Act proposes the establishment of a *Data Protection Board of India*, an independent adjudicatory body responsible for enforcing compliance. While the Act outlines monetary penalties for non-compliance, concerns remain about the actual independence and capacity of the Board. Moreover, the broad exemptions for government agencies could potentially undermine the enforceability of data subject rights[10].

In contrast, the US model lacks a central enforcement authority for data protection. The *Federal Trade Commission (FTC)* plays a pivotal role, particularly through its authority to regulate "unfair or deceptive practices." However, enforcement largely relies on post-facto remedies and settlement negotiations, rather than proactive oversight. The state of California has recently established the *California Privacy Protection Agency (CPPA)*, but this remains a state-level body with no federal equivalent.[276]

Cross-border data transfers are another critical area of divergence. The GDPR permits such transfers only to jurisdictions that offer an "adequate level of protection," or under safeguards such as *Standard Contractual Clauses (SCCs)* or *Binding Corporate Rules (BCRs).* After the invalidation of the US-EU Privacy Shield in the *Schrems II* decision, transatlantic data transfers have become increasingly complex.[277]

---

[275] GDPR, art 5(1)(b)
[276] California Privacy Protection Agency, *About CPPA* https://cppa.ca.gov accessed 12 May 2025
[277] Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems [2020] ECLI:EU:C:2020:559

India, under the DPDP Act, envisions restrictions on cross-border transfers, particularly for "critical personal data," which must be stored and processed only in India. The government retains the power to specify countries where data transfers may be permitted, creating a discretionary and possibly protectionist framework. The US, in contrast, favours unrestricted data flows and generally does not impose localisation requirements, which has been a point of contention in global trade negotiations.

CHALLENGES IN IMPLEMENTATION AND REGULATORY GAPS

STRUCTURAL, INSTITUTIONAL, AND JURISDICTIONAL BARRIERS

While the legal architecture of data protection laws in India, the EU, and the US appears robust on paper, their implementation has been challenged by systemic, institutional, and jurisdictional gaps that often hinder their effectiveness. A key concern across jurisdictions is the *mismatch between legislative ambition and enforcement capability*.

In the EU, despite having a well-developed regulatory framework through the General Data Protection Regulation (GDPR), implementation varies significantly across member states. Many *Data Protection Authorities (DPAs)* face resource constraints, leading to selective enforcement and procedural delays.[278] The complexity of cross-border cases, which require cooperation between multiple DPAs under the GDPR's one-stop-shop mechanism, often results in protracted investigations and inconsistent interpretations of the law.[279] Moreover, powerful multinational corporations based in non-EU countries continue to test the limits of EU jurisdiction, raising concerns about the enforceability of GDPR provisions on foreign soil.[280]

In India, the newly enacted *Digital Personal Data Protection Act, 2023 (DPDP Act)* presents significant implementation challenges. The lack of a pre-existing enforcement ecosystem, combined with a vast and diverse digital economy, complicates effective rollout. The proposed *Data Protection Board of India* is yet to be operational, and its actual independence from executive control remains a concern.[281] Furthermore, the DPDP Act provides broad exemptions to the state under grounds such as national security, public order, and sovereignty. These exemptions may be invoked frequently, thereby weakening the scope of judicial or regulatory scrutiny and potentially undermining citizens' privacy rights.[282]

---

[278] European Data Protection Board, *Annual Report 2022* https://edpb.europa.eu accessed 10 May 2025
[279] GDPR, arts 60–63
[280] Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Law' (2015) 5(4) International Data Privacy Law 235
[281] Digital Personal Data Protection Act 2023 (India), s 19
[282] *Ibid*, s 17

The US faces a different but equally pressing set of problems. Its *sectoral approach*, where data protection is regulated by industry-specific laws, creates a fragmented landscape. This fragmentation results in inconsistent standards, overlapping jurisdiction among federal and state regulators, and significant loopholes for companies operating across multiple sectors.[283] The lack of a comprehensive federal law also complicates efforts to enforce data rights at a national level. Although the *Federal Trade Commission (FTC)* is the de facto privacy regulator, its authority is limited to consumer protection rather than dedicated data rights enforcement. Additionally, pre-emption debates have hindered efforts to pass uniform legislation, with states like California, Virginia, and Colorado enacting their own comprehensive privacy laws.[284]

TECHNOLOGICAL EVOLUTION AND ENFORCEMENT FATIGUE

Another significant challenge lies in the rapid evolution of technology outpacing regulatory capacity. Emerging technologies such as artificial intelligence (AI), machine learning, big data analytics, and biometric surveillance systems increasingly pose threats to the privacy and autonomy of individuals. Laws that were crafted to regulate basic data processing are now being applied to *automated decision-making systems* that can produce discriminatory or opaque outcomes, raising fresh regulatory dilemmas.[285]

The GDPR attempts to address this through Article 22, which restricts decisions based solely on automated processing. However, the enforcement of this provision remains weak, with ambiguities in interpretation and limited case law. Moreover, as AI becomes increasingly central to business operations, companies often argue that such decisions are not "solely automated," thereby avoiding regulatory oversight. In India, the DPDP Act does not explicitly address automated processing or profiling, representing a significant legislative gap at a time when surveillance technologies are increasingly used for governance, policing, and welfare delivery.[286]

In the US, there is a growing movement towards regulating algorithmic decision-making, but legislation is still at a nascent stage. While the *Algorithmic Accountability Act* has been introduced in Congress, it is yet to be enacted. The existing laws, such as the CCPA, offer

---

[283] Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (2015) 83 Geo Wash L Rev 2230

[284] California Consumer Privacy Act 2018; Virginia Consumer Data Protection Act 2021; Colorado Privacy Act 2021

[285] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76

[286] Internet Freedom Foundation, 'Analysis of the Digital Personal Data Protection Bill, 2022' (2022) https://internetfreedom.in accessed 11 May 2025

limited protection against profiling or algorithmic bias, and enforcement is largely reliant on public interest litigation or media scrutiny rather than proactive regulatory oversight.[287]

Enforcement fatigue is another emerging issue, particularly in the EU. Since the introduction of the GDPR, the volume of complaints has increased significantly, straining the capacity of regulatory authorities. Many smaller companies find compliance to be financially and administratively burdensome, resulting in either *superficial compliance* or outright non-compliance, especially in countries with weaker enforcement records.[288] This leads to uneven regulatory landscapes within the EU itself and undermines the promise of uniform protection.

Similarly, in India, the lack of awareness about digital rights, low digital literacy, and inadequate access to legal remedies severely limit the practical enforceability of the DPDP Act's provisions. For many citizens, *filing a complaint or seeking redress* is simply not a viable option. Additionally, India's heavy reliance on digital public infrastructure like Aadhaar makes the state both a key data fiduciary and a potential violator of data privacy norms.[289]

The private sector also plays a crucial role in implementation. While large multinational corporations often have compliance departments and legal teams to navigate data protection regimes, small and medium enterprises (SMEs) struggle with compliance due to costs and lack of expertise. This is particularly true in India and the US, where legal obligations vary significantly across sectors and jurisdictions. For instance, an SME operating in both New York and California may be subject to *entirely different data protection requirements*, increasing legal uncertainty and administrative burdens.[290]

In conclusion, implementation challenges across India, the EU, and the US are shaped not only by legal design but also by political will, administrative capacity, technological complexity, and socio-economic realities. While the GDPR remains the most comprehensive regime in principle, its effectiveness depends heavily on consistent enforcement across member states. The US's fragmented system remains riddled with inconsistencies, and India's new regime must address significant structural and institutional challenges before it can fully protect digital privacy. The next and final chapter will consider future directions and possible frameworks for harmonising global data protection standards.

---

[287] Algorithmic Accountability Act, S.1108 (2022), 117th Congress

[288] Graham Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 Privacy Laws & Business International Report 1

[289] Usha Ramanathan, 'Aadhaar and the Right to Privacy' (2018) 2(1) Indian Journal of Law and Technology 4

[290] Jules Polonetsky, Omer Tene and Joseph Jerome, 'Benefit-Risk Analysis for Big Data Projects' (2014) 7(2) International Data Privacy Law 103

FUTURE DIRECTIONS AND THE CASE FOR GLOBAL HARMONISATION

TOWARDS CONVERGING STANDARDS IN DATA PROTECTION

As digital technologies become increasingly global in reach and operation, the *disparate nature of data protection laws* poses serious challenges for cross-border governance, business compliance, and the protection of fundamental rights. The comparative analysis of India, the EU, and the US reveals a significant *lack of coherence*, not only in legislative design but also in enforcement mechanisms and underlying philosophies. This divergence underlines the growing need for *convergence and harmonisation* of data protection standards at the international level.

One promising development is the emergence of the *EU's GDPR as a global benchmark*. Several countries, including Japan, South Korea, Brazil, and South Africa, have either adopted GDPR-inspired legislation or entered into adequacy agreements with the EU.[291] Even corporations based in jurisdictions with weaker protections, such as the US, are increasingly aligning their internal data governance frameworks with the GDPR to ensure global compliance.[292] The *"Brussels Effect"*, wherein EU regulatory norms influence global standards due to market power and extraterritorial applicability, has played a crucial role in shaping the global conversation on privacy.[293]

India's *Digital Personal Data Protection Act, 2023*, reflects partial alignment with the GDPR, particularly in its emphasis on user consent, purpose limitation, and accountability. However, the legislation falls short in key areas such as restrictions on government access, algorithmic transparency, and the absence of a strong, independent regulatory authority. To truly achieve convergence, India must strengthen procedural safeguards and align with *international best practices*, particularly as it seeks to expand its digital economy and engage in global data partnerships.[294]

In the US, pressure is mounting for the adoption of a *comprehensive federal privacy law*. The increasing number of state-level statutes, such as the California Consumer Privacy Act (CCPA), has created a fragmented legal environment that is both inefficient and inequitable. A federal framework modeled on GDPR principles—such as data minimisation, accountability, and data subject rights—could not only streamline compliance for businesses but also protect

---

[291] Graham Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 Privacy Laws & Business International Report 1

[292] Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94(4) NYU L Rev 771.

[293] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020)

[294] Internet Freedom Foundation, 'Analysis of the Digital Personal Data Protection Bill, 2022' https://internetfreedom.in accessed 12 May 2025

American citizens more effectively in the digital age.[295] However, debates over *pre-emption and private right of action* remain key stumbling blocks to consensus in Congress.[296]

PROSPECTS FOR INTERNATIONAL COOPERATION AND REGULATORY INNOVATION

Efforts toward global harmonisation must also address the role of *multilateral forums* such as the *Organisation for Economic Co-operation and Development (OECD)***,** *United Nations (UN)*, and *G20*, which have the potential to create soft law frameworks or model regulations for data governance. The OECD Privacy Guidelines, originally issued in 1980 and updated in 2013, continue to serve as a reference point for national legislation, promoting principles of fairness, security, and individual participation.[297] However, these guidelines lack binding force and depend on voluntary implementation.

The *G20 Osaka Leaders' Declaration (2019)* introduced the concept of "Data Free Flow with Trust" (DFFT), which seeks to balance economic growth with strong data protection safeguards. Although still in the formative stage, DFFT provides a platform for dialogue and cooperation between countries with different legal systems and values.[298] India, the EU, and the US all participate in G20 deliberations, offering a strategic opportunity to develop shared frameworks for cross-border data flows.

Another key avenue for convergence lies in *bilateral and regional agreements***.** The EU-US "Privacy Shield" framework—struck down in *Schrems II*—has been followed by the *Trans-Atlantic Data Privacy Framework*, a proposed mechanism for enabling compliant data flows while addressing concerns over US surveillance laws.[299] Similarly, India is negotiating data transfer arrangements with several jurisdictions to ensure reciprocal protection and facilitate trade. The future of such arrangements will depend on aligning domestic laws with international expectations regarding surveillance, redress mechanisms, and judicial oversight.

In parallel, regulatory innovation through *technological solutions* such as *privacy-enhancing technologies (PETs)***,** *data trusts*, and *differential privacy mechanisms* could help bridge the enforcement gap. These technologies allow data processing to occur in ways that minimise individual identifiability, thereby aligning with the spirit of data protection laws while

---

[295] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018)

[296] Cameron F Kerry, 'Why the US Needs a Comprehensive Federal Privacy Law' (Brookings, 2021) https://www.brookings.edu accessed 13 May 2025

[297] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).

[298] G20, *Osaka Leaders' Declaration*, 28–29 June 2019 https://g20.org accessed 13 May 2025

[299] Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems [2020] ECLI:EU:C:2020:559

facilitating innovation.[300] Governments, particularly in India and the US, can leverage these tools to improve compliance outcomes, especially in the public sector where large-scale data processing is common.

Finally, public awareness, digital literacy, and civil society engagement will be crucial for the long-term sustainability of any data protection regime. In all three jurisdictions, privacy must move beyond elite legal discourse and become part of the broader public consciousness. Education, advocacy, and access to redress mechanisms must be made universally available to empower individuals to assert their rights in a complex and data-driven world.

CONCLUSION

The comparative study of India, the EU, and the US underscores that while each jurisdiction has made strides in data protection, *none has achieved a perfect balance* between rights, innovation, and enforcement. The GDPR offers the most comprehensive model, but its extraterritoriality and enforcement challenges highlight the need for global cooperation. India's DPDP Act is a welcome step forward but must overcome structural and normative limitations. The US must move beyond its fragmented, market-centric approach to embrace a rights-based, federal framework. As data becomes the defining asset of the digital age, the need for **a** *harmonised, equitable, and enforceable global data protection architecture* is more urgent than ever. International cooperation, legislative reforms, and technological innovation must converge to build a system where privacy is respected across borders and across platforms.

[300] Mireille Hildebrandt, 'Privacy as Protection of the Incomputable Self' (2011) 1(1) IDPL 1