CROSS-BORDER DATA PRIVACY AND JUSTICE: RECONCILING NATIONAL LAWS WITH GLOBAL DIGITAL REALITIES

Charu Singh, IILM, Greater Noida

ABSTRACT

The globalization of digital technologies has transformed personal data into a fluid, borderless resource, challenging the traditional jurisdictional boundaries of national legal systems. While states continue to regulate privacy through territorially grounded frameworks such as the GDPR, CCPA, and India's DPDP Act, the inherently transnational movement of data generates legal conflicts, regulatory uncertainty, and uneven levels of rights protection. This paper examines the justice gap that arises from this fragmentation, analyzing how divergent national standards shape the governance of cross-border data flows. Through a comparative study of major data protection regimes and an evaluation of judicial interventions—including *Google Spain*, *Schrems I*, and *Schrems II*—the research highlights the growing role of courts in mediating privacy disputes within a global digital ecosystem. The paper also assesses emerging international initiatives by the OECD, Council of Europe, APEC, and the United Nations that aim to establish interoperable principles for global data governance. Despite these efforts, geopolitical tensions, digital sovereignty claims, and power asymmetries between states and technology corporations continue to obstruct meaningful harmonization. The study argues that a just and effective cross-border data regime requires globally interoperable standards, equitable participation for developing countries, and stronger international enforcement mechanisms. It concludes that a rights-based, cooperative approach is essential for reconciling national laws with the realities of global digital interconnectivity.

Keywords: Cross-border data privacy; digital sovereignty; GDPR; global data governance; surveillance; Schrems; right to be forgotten; international cooperation; digital justice; data protection frameworks.

1. INTRODUCTION: DATA AS A BORDERLESS RESOURCE

The terrific increase in digital technologies has radicalized data into an open source that circulates across jurisdictions freely with ease. The social media, cloud computing applications, e-commerce in the form of multinational and even the daily cross-border exchange of personal information with the user explicit or not[1]. In this globalized digital ecosystem, the data is not limited by the borders of the territory of one particular country; it flows through a complicated system of server, data centres, and corporate structures located in a number of different countries. This lack of geographical location of data essentially contests the conventional concept of sovereignty, in which legislation is traditionally more geographically confined in the past.This nondomesticity of information is the major force that challenges the traditional definition of sovereignty, when legislation had been geographically restricted in the past.

Although data is acting as a transnational commodity, national laws remain territorially based. As one example, the General Data Protection Regulation (GDPR) of the European Union provides strong requirements even to foreign entities that process the data of the citizens of the EU, which proves the extraterritorial aspirations of the national laws. Other jurisdictions include the United States which is sectoral and business-friendly by other jurisdictions and most developing economies have fragmented or weak privacy laws. Such a regulatory difference causes tension at the border between the global streams of data and local regulations on privacy, accountability, and the rights of users, which results in the inconsistency of privacy, accountability, and user rights standards.[2]

Privacy has therefore become one of the key justice issues of the international digital age. Citizens are finding themselves more vulnerable to threats of surveillance, misuse of data, and profiling with algorithms, and transfer of their personal information to other countries without their permission[3]. Data transmitted across borders mean that the legal protections afforded to individuals will be based on the location of data processing and not the location of residence of the individual- creating a huge disparity between the citizens of two different nations. The issue of this justice gap is especially problematic to people in the Global South, where the data protection regimes can underdeveloped or poorly enforced, leaving millions of people at a

[1] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
[2] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).
[3] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).

disadvantage to exploitation by international technology companies.

It is in this context that the fundamental research issue of the paper is the increasing disjointedness in law concerning the protection of privacy of nationwide data and how current legal frameworks are unable to adequately regulate the naturally transnational flow of information. Lack of a unified international system creates a lack of legal certainty, jurisdictional source, as well as inconsistency in the protection of rights, thus being detrimental to the privacy of the individual as well as to the sovereignty of states[4].

This research will involve the analysis of key national regimes concerning data protection, judicial involvement, comparative legal frameworks and the investigation of international efforts to regulate the data management across the borders. The paper is framed by some of the most important research questions, such as:

1.What is the clash between national data privacy legislation and the borderless digital data?

2.What is the role of courts in providing solutions to the conflicts that emerge due to cross-border data transfer?

3.How can a unified international system be developed with the help of what models or principles?

4.What is the solution of global digital order between individual rights and state sovereignty?

The research methodology to address these questions is a doctrinal approach, and the research involves statutory frameworks, court opinions, and commentaries. It also applies the comparative analysis to assess the disparity between major regimes in the GDPR, CCPA and the Indian data protection law. In addition, a case based method such as landmark litigation such as Google Spain v. AEPD and Schrems I and II - aid in understanding how the courts balance the jurisdiction laws with international data flow generation[5]. The joint approaches allow a holistic insight into the justice issues that are rooted in cross-border data privacy regulation.

[4] Paul M. Schwartz, "Global Data Privacy: The Conflict Between EU and US Privacy Law," *Minnesota Law Review*

[5] *Google Spain SL v. AEPD*, Case C-131/12, Court of Justice of the European Union (2014); *Schrems v. Data Protection Commissioner*, Case C-362/14 (CJEU 2015); *Schrems II*, Case C-311/18 (CJEU 2020).

2. FRAGMENTED NATIONAL FRAMEWORKS & REGULATORY CONFLICTS

The international data privacy is largely complex due to the disjointed nature of the national law on its governance. Despite the routine blurring of territorial borders by digital interactions, the majority of data protection laws are still based on the Westphalian paradigm of state sovereignty that imposes conflicting and overlapping regulatory requirements. The most powerful of the regimes, the General Data Protection Regulation (GDPR) of the European Union, establishes a high level of data protection and has a strict compliance rate of any organization processing the data of the EU residents, irrespective of the location of the organization. This extraterritoriality has redefined the world wide data governance as companies across the world have been forced to implement GDPR level of protection in order to evade fines[6]. Conversely, the United States is a decentralized, sector-regulated system, in which privacy regulations do not exist universally but differ by industry, including healthcare, finance, and online data of children, and it does not have a unified, federal privacy law. The model is associated with the market-driven philosophy of the country and makes an acute contrast with the European rights-based approach, which is market-driven as well[7].

The upcoming economies also create the additional global legal scene. The Digital Personal Data Protection Act (DPDP Act) of India proposes liability in terms of consent, limitation of purpose, reporting on data breaches, but its liability framework remains in its early stages, and the legislation on cross-border data transfer is still being modified to better reflect new market trends[4]. Other nations like Brazil (LGPD), South Africa (POPIA), and Singapore (PDPA) have embraced hybrid models in the pursuit of striking a balance between economic growth and data protection, but they vary in the area covered, the intensity, and the ability to enforce them. This variety leads to the inequality of the world, as the same data set can be securely stored in one nation and be unprotected in another, depending on the law that regulates it[8].

These differences result in direct regulatory clashes in situations where the multinational companies handle, or transfer data between jurisdictions. As an illustration, a company that is based in the EU, the US, and India at the same time has conflicting needs on the consent

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
[7] Daniel J. Solove & Woodrow Hartzog, "The Omission of the Federal Privacy Law in the United States," *Harvard Law Review* (2021).
[8] Danilo Doneda & Miriam Wimmer, "Brazil's General Data Protection Law: A Detailed Overview," *International Data Pvacy Law* (2019).

standards, user rights, data storage requirements, and breach notification schedules.[|human|>To provide an example, a company, which is located in the EU, the US, and India concurrently, has contradictory requirements with regard to consent standards, user rights, data storage requirements, and breach notification timelines. The GDPR requires explicit, informed consent and provides rights including erasure and portability, whereas the US laws do not need to provide privacy notices and have no privacy rights. The DPDP Act of India proposes consent-based processing but gives the government exemptions, which may contradict the standards of adequacy in the GDPR. These differences make it difficult to comply, make it more expensive to administer, and generate legal confusion on corporations that are involved in international activities.

Moreover, even national policies of data localization and cross-border transfers conflict influence regulatory friction. Countries like China, Russia or India have been focusing more on the notion of digital sovereignty by enacting the data localization laws that compel some types of personal or sensitive information to be locally stored within a country[9] These are aimed at enhancing state control, providing security and promoting local enforcement but is directly opposing the EU streamlined cross-border transfer mechanisms that are based on adequacy determinations or standard contractual terms. Without internationalized standards, the unilateral data control solutions of the nations continue to divide the legal environment further, compromising the smooth operation of the digital markets.

The overall impact of this disintegration is increased justice gap. People get different levels of privacy protection by different routes that their data takes, and companies are exposed to conflicting responsibilities, which can not be fulfilled at the same time[10]. In the absence of an international framework, cross-border data regulation is a system of inconsistent rules and regulations, which creates regulatory arbitrage, forum shopping and diminished accountability. This section thus highlights the importance of coming up with interoperable structures that can counter the national legal divergence in an international digital world.

3. GEOPOLITICS, SOVEREIGNTY & POWER ASYMMETRY IN DATA GOVERNANCE

The control of the cross-border data flows is now not a privacy and technical regulation issue

[9] Christopher Kuner, "Data Localization Trends and Challenges," *International Data Privacy Law*.
[10] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014).

any longer, it has become a geopolitical issue that defines the world order of power. States are recognizing data as one of their strategic assets, which are important in national security, economic competitiveness, and political independence. This has fuelled discussions on the concept of digital sovereignty, that is, nations are trying to exercise control over data that is created on their territories, although processed or stored on other countries. The pressure between international information flows and the statehood has led to complicated governance battles, where influential nations and tech giants determine the regulations of the online environment. Cross-border data regulation, in this case, gets strongly interwoven with geopolitical interests, the issue of cyber security, and the global competition in terms of technological supremacy[11].

There have been some nations, especially China and Russia, which have implemented strict data localization legislation due to the fear of foreign surveillance, cyber-espionage and political manipulation. Such steps demand the personal or sensitive data to be stored on-site and usually limit the international transfer without meeting the conditions that are set by the government[12]. Although these types of laws increase the power of the state and ensure direct access of domestic security agencies, they also bring the problem of censorship, human rights considerations, and decreased digital transparency. Western democracies, on the other hand, propose a rights-based approach and conditional data transfers on the basis of adequacy, safeguards and rule of law commitments[13]. These contrasting models demonstrate how the geopolitical philosophies influence the models of data governance: authoritarian-regulatory models involve more emphasis on state control whereas liberal-democratic states focus on the rights of individuals and the stability of the market.

There is also a big geopolitical conflict between Big Tech corporations and the governments with power. Google, Meta, Amazon and Apple are corporations that handle large volumes of data that are many times more than many nation-states, which gives them unprecedented control over digital infrastructures. With their presence worldwide, they are able to cross over boundaries and influence the practice of the enforcement of privacy norms. This leads to a power imbalance: the developed nations have the opportunity to engage in negotiation with

[11] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).
[12] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).
[13] Anita Gurumurthy & Parminder Jeet Singh, "Digital Colonialism: South–North Power Relations in the Data Economy," *IT for Change* (2020).

Big Tech on the same terms, whereas most developing nations do not have the economic and political resources to make Big Tech comply, leading to a skewed privacy and regulation practices and becoming reliant on Big Tech regulation.< This difference is another kind of digital colonialism where nations of the Global South are made into data mining locations without sufficient control over the information gathered and utilized, or monetization of the information about their citizens.

These geopolitical boundaries are also reflected in the international negotiations. The attempts of creating global data governance systems, including those offered by the United Nations, OECD, and G20, are often undermined by national security concerns, economic interests, and ideological variations in national interests and values[14]. The developed technological countries demand free data flows to give their online industries a boost, and the developing economies demand more protection and state-sovereign controls to prevent technological dependence. Lack of geopolitical convergence results in a disconnect between harmonization of data protection standards that consequently results in a disjointed global standard, and discrepancies in protection of individuals whose data is transferred across borders.

The compound effect of such power imbalances is the expansion of the justice gap in the global data governance. The people in the jurisdictions which have a poorer regulatory ability or a geopolitical footprint stand a higher risk of privacy breaches, algorithm manipulation, and discrimination based on data.[15] At the same time, hegemonic states and companies keep dictating the terms of data cross-border flows, which strengthens the unequal power balance. It is crucial to the conceptualization of a just digital order to understand these geopolitical tensions and make sure that the data governance does not replicate global inequalities and respect both state sovereignty and individual rights.

4. JUDICIAL DIMENSION: COURTS SHAPING CROSS-BORDER PRIVACY NORMS

The courts are now an enormous platform of dispute concerning international data flow, especially at the point where the national legislation overlaps international digital practices. The jurisdiction courts are facing an increment in cases of foreign data transfer, issues of surveillance and extraterritoriality of privacy laws. These judicial interventions demonstrate

[14] OECD, *Privacy Guidelines and Cross-Border Flows of Personal Data* (2013).
[15] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014).

the underlying conflict between the territorially bound legal requirements and global flow of personal data.[16]. Courts in their interpretations do not only serve in resolving disputes but also shape the changing architecture of global data governance, frequently taking gaps created by legislatures that cannot keep up with technological change.

The case that caused one of the most significant judicial interventions affecting privacy across the borders is Google Spain v. by the Court of Justice of the European Union. AEPD, which cited the right of being forgotten. The court stated that the search engines that work around the world should adhere to the EU privacy standards when handling the personal information of the EU citizen[17]. This case law was a significant extension of the extraterritorial scope of the GDPR prior to its formal implementation and an indication of how the judiciary is open to interfering with global privacy principles by imposing regionalization values. The ruling also highlighted the way in which courts might also take an active role in re-establishing digital rights across the national boundaries.

On the same note, both the Schrems I (2015) and Schrems II (2020) rulings significantly transformed the environment of transfers of EU data to the US. In Schrems I, the CJEU struck down the agreement on the "Safe Harbor" declaring that US surveillance practices could not be reconciled with the standards of fundamental rights in the EU[18]. The case of the same was overruled, Schrems II, five years later, on the basis of the same factors, on the insufficiency of the protections against unwarranted surveillance of states of the US. The decisions revealed weaknesses in the structure of data transfer systems and transatlantic operations and highlighted the importance of the courts as privacy-conscious guardians in the context of geopolitics.

Indian judiciary has also helped in the indirect development of the cross-border data norms. Justice K.S. Puttaswamy v. [1948] A.C.511. In the case of Union of India, the Supreme Court stated that privacy is a fundamental right under Article 21 of the Constitution[19]. Despite the fact that the decision did not explicitly touch upon the issue of cross-border data flows, its acknowledgment of privacy as a part of personal liberty has impacted on the discussions concerning international data transfer, data localizations, and the creation of the Indian data

[16] Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal*
[17] *Google Spain SL v. AEPD*, Case C-131/12, Court of Justice of the European Union (2014).
[18] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Case C-311/18 (CJEU 2020).
[19] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006)

protection laws. The judiciary has also become active in enforcing rights-based data regulations by compelling state authorities, and other entities, to justify their data processing undertakings by courts under constitutional review.

Nevertheless, the jurisdiction of the courts in the field is subject to the territorial boundaries of the national laws. Courts cannot solve global governance problems like inequalities in national regimes on surveillance, lack of uniformity in data transfer rules or inconsistent standards of user rights on their own in isolation. Judgments with global impacts, as happened in the CJEU decisions, are subject to limited application to the extent of indirect impact of market power or spillover effects of regulation. The absence of a consistent global system of international law tends to force domestic courts to resolve transnational cases through national legislation that was not modeled after the complexity of global data ecosystems.

However, the overall consequence of judicial activism is that it has exposed how insufficient current international systems are and the necessity to have more robust and unified provisions to protect the data that is being moved across international borders. These judicial rulings have caused governments to renegotiate data transfer agreements, prompted legislatures to make domestic privacy laws more robust, and prompted corporations to implement more stringent compliance mechanisms[20]. By doing so, courts will be both empowering and constraining units- they will act as agents of change and yet will act within the parameters of national jurisdiction. Their changing jurisprudence is a pivotal aspect of the global quest to bring data privacy and the reality of an increasingly digitally connected world into a harmonized state.

5. EMERGING INTERNATIONAL AND MULTILATERAL RESPONSES

The fragmented global landscape of data protection has pushed several international and multilateral bodies to articulate frameworks that promote a more coherent approach to cross-border data governance. Although no universal treaty on data privacy exists, a patchwork of international guidelines, principles, and cooperative initiatives has begun shaping normative expectations for states and corporations operating across borders. These efforts reflect the growing recognition that the global nature of digital technologies requires correspondingly global solutions that go beyond the jurisdictional limitations of national laws. The international

[20] Christopher Kuner, "The Jurisprudence of the CJEU on International Data Transfers," *International Data Privacy Law*

community increasingly acknowledges that a harmonized, rights-based system is necessary to prevent legal conflicts, promote fairness, and ensure accountability in cross-border data flows.

One of the most influential international instruments in this sphere is the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, originally adopted in 1980 and updated in 2013. These guidelines introduced foundational privacy principles such as purpose limitation, data quality, security safeguards, and accountability, which have since influenced legislation worldwide.Although non-binding, the OECD framework has served as a soft-law template for many countries, particularly those seeking to modernize their data protection regimes while maintaining compatibility with global economic systems. Similarly, the Council of Europe's Convention 108 remains the only binding international treaty on data protection, offering a rights-centric approach that has been ratified by countries within and beyond Europe. Its modernization through Convention 108+ further aligns international expectations on cross-border transfers and supervisory cooperation.

The United Nations has also taken steps toward global digital governance, particularly through the UN High-Level Panel on Digital Cooperation and ongoing negotiations around the Global Digital Compact. These initiatives emphasize human rights, digital inclusion, and cross-border interoperability as essential components of a fair digital order.[21] While these efforts do not yet constitute a binding regime, they reflect a growing convergence on the need for international standards that address power imbalance between states and dominant technology corporations. Moreover, UN human rights bodies increasingly frame data privacy as integral to the rights to dignity, autonomy, and freedom from arbitrary surveillance, thereby expanding the normative foundation for global privacy governance.

Other international groupings such as the G20, APEC, and the African Union have also developed frameworks promoting cross-border data cooperation. The APEC Cross-Border Privacy Rules (CBPR) system is particularly notable as a voluntary mechanism allowing businesses to transfer data across participating jurisdictions while meeting baseline privacy requirements.[22] Although less stringent than the GDPR model, the CBPR system represents an important effort at building interoperability without imposing uniformity. Regional initiatives such as the African Union Convention on Cybersecurity and Personal Data Protection similarly

[21] United Nations, *Report of the Secretary-General's High-Level Panel on Digital Cooperation* (2019).
[22] APEC, *Cross-Border Privacy Rules (CBPR) System* Framework.

signal a shift toward structured governance in regions historically underrepresented in digital policy discourse.[23]

Despite these emerging initiatives, significant challenges remain in establishing global harmonization. Geopolitical tensions—particularly among major digital powers such as the European Union, China, and the United States—complicate consensus-building on issues like surveillance, data localization, and national security exceptions. Additionally, the voluntary nature of most international frameworks limits enforceability, leaving compliance largely dependent on political will and economic incentives[24] This creates gaps in accountability, especially in regions where regulatory institutions are weak or where governments prioritize security and economic interests over privacy rights.

Nevertheless, these international and multilateral efforts represent an important step toward a more coherent global data governance architecture. They provide normative foundations that can guide states in reconciling domestic privacy laws with global digital realities and in negotiating future binding agreements. As technological development accelerates, the need for interoperable standards and shared commitments becomes increasingly urgent to ensure that cross-border data flows occur within an equitable, rights-protective framework.[25]

6. TOWARD A JUST AND HARMONIZED CROSS-BORDER DATA REGIME

The growing sophistication of international flows of data highlights the pressing necessity of a state-of-the-art and justice-centered system of cross-border privacy management. With the flowing data on the borders of nations, the national laws are in trouble in giving sufficient protection or uniformity of standards in the countries which have been drafted in the context of traditional sovereignty. The international justice regime should thus be able to balance a borderless digital information with the territorial basis of legal jurisdiction. This type of regime does not just depend on legal interoperability among states, but a shared interest in protecting individual rights regardless of geography**[26]**. The main issue here is how to build a model that would accommodate the competing interests on privacy, innovativeness, national security, and

[23] African Union, *Convention on Cyber Security and Personal Data Protection* (2014).
[24] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).
[25] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).
[26] Paul M. Schwartz, "Global Data Privacy: The Conflict Between EU and US Privacy Law," *Minnesota Law Review*

economic development without recreating the power disparities in the world.

The main element of a harmonized data regime is the creation of interoperable privacy norms that would enable various legal regimes to operate together without standardization. Interoperability seeks to establish shared minimum protection mechanisms like clear consent, use of purpose, minimization of data, and the transfer mechanisms with clarity in addition to allowing individual jurisdictions to uphold their own philosophy of regulation[27]. Such standards would be of help to companies that operate in several regions, minimize conflicts of law, and give more security to individuals as to their rights in case their data crosses a border. The OECD Guidelines, Convention 108 + and the APEC CBPR framework, which is not flawless, show that flexible, principle-based harmonization can be effective in a variety of legal systems.

Other pillars of a just global regime are the enhancement of international supervisory and enforcement systems. The existing frameworks are highly dependent on domestic authorities and there is a huge form of inconsistency in regulatory capacity between nations. An even more fair model would allow collaboration between data protection agencies, ease international investigations and offer tools to conduct collaborative enforcement measures[28]. The absence of such joint enforcement implies that strong technological companies have an opportunity to use jurisdictional loopholes, and states that lack resources might fail to bring them to justice. An increase in international cooperation would thus promote the protection of privacy as well as the sovereignty of the weaker states. Besides, a just cross-border data architecture should cover current power imbalance in the world digital order. The Global South countries are disadvantaged structurally, such as low bargaining power to enter into data transfer agreements, inadequate technological infrastructures, and being exploited digitally. In order to avoid the digital colonialism, any harmonized model shall include equal participation, capacity-building efforts together with protection of the fact that developing countries will be able to participate in the global rule-making processes[29]. The concept of justice in the global digital neighborhood will not be fulfilled when the harmonization only copies the already existing hierarchies by introducing new standards that were primarily created by the regions, which are technologically

[27] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).
[28] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).
[29] Anita Gurumurthy & Parminder Jeet Singh, "Digital Colonialism: South–North Power Relations in the Data Economy," *IT for Change* (2020).

advanced.

The reinstatement of data privacy as a human right is one of the key pillars of a just international regime. The international communities, such as the United Nations, have stressed the necessity to safeguard information against unjustified surveillance, discriminatory algorithmic operation, and manipulative business procedures[30]. A rights-based paradigm means that the core of cross-border governance is the individual autonomy, dignity, and agency, even when the data is being processed by foreign companies or handed over to the jurisdictions with another legal philosophy. This moral basis enhances legitimacy of future governance systems and establishes responsibility of states and other non state actors.

Clear and responsible mechanisms of data transfer are also needed to implement a harmonized cross-border regime. Adequacy determinations, standard contractual clauses and certification systems need to be created or revised to include greater prevention of foreign surveillance, metadata tracking, and state overreach[31]. Schrems I and Schrems II teach us the necessity of making sure that the arrangements of data transfer observe human rights and offer efficient remedies. In the absence of such measures, harmonization will be a formalistic exercise that does not have substantive guarantees.

Finally, to realize a fair and balanced international data regime requires long-term international collaboration, political goodwill and understanding of data as a universal issue. The strictly national strategy is no longer an option: the digital world needs common structures of governance that would help safeguard the rights, which respect the sovereignty, and provide international interoperability. Although harmonization might not lead to an immediate single binding treaty, there can be gradual steps, by the process of multilateral negotiations, regional structures, and international standard-setting, to a more fair base structure. The international community can also take a step toward a more human-centric framework of cross-border data governance by filling in the divide between national regulatory frameworks and the global digital realities.

CONCLUSION

The global circulation of data has exposed deep structural tensions between the borderless

[30] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Case C-311/18 (CJEU 2020).
[31] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014)

nature of digital information and the territorially anchored frameworks of national law. As the analysis across this paper has shown, fragmented regulatory regimes, geopolitical rivalries, and power asymmetries between states and technology corporations create significant gaps in justice, accountability, and individual rights protection. While national laws like the GDPR, CCPA, and India's DPDP Act attempt to regulate privacy within their own jurisdictions, none of them alone can adequately address the challenges posed by data that constantly moves across borders.

Judicial interventions—from *Google Spain* to the *Schrems* decisions—have played an important role in advancing privacy protections, but courts remain constrained by domestic mandates and cannot resolve the deeper international inconsistencies on their own. At the same time, global and regional initiatives led by bodies such as the OECD, the Council of Europe, APEC, and the United Nations represent early steps toward building a more coherent international data governance architecture. Yet these efforts are still evolving, often voluntary, and frequently hampered by geopolitical disagreements and differing national priorities.

For the international community, the path forward lies in creating harmonized, interoperable standards that respect both individual rights and state sovereignty. A just global data governance framework must ensure equitable participation for developing countries, provide effective oversight and enforcement mechanisms, and recognize privacy as a fundamental human right in the digital age. Ultimately, achieving this balance requires sustained multilateral cooperation, political commitment, and the acknowledgement that data is not merely an economic asset or a tool of state security, but a critical dimension of human autonomy and dignity.

A truly fair cross-border data regime will emerge only when nations collectively embrace the idea that digital rights transcend borders. By bridging the divide between national legal systems and global digital realities, the world can move toward a more inclusive, rights-based, and trustworthy digital order—one that upholds justice for every individual, regardless of where their data travels.