Sarhad Journal of Legal Studies

July-December 2025, Vol. 01, No. 02, [01–09]
Published: 31st July 2025
Publisher: Sarhad Institute of Legal Studies, SUIT
https://journal.suit.edu.pk/index.php/sjls

RESEARCH PAPER

Cross-Border Data Flows and Privacy Rights: Reconciling International Norms with National Security

Muhammad Atif Khokhar[1]*

ABSTRACT

The rapid growth of digital technologies and globalization has made cross-border data flows a key driver of economic growth, innovation, and governance. However, these flows raise significant concerns over privacy and national security, creating tensions between international norms and domestic regulations. This study explores legal and policy frameworks governing cross-border data transfers, including international agreements like the EU–US Data Privacy Framework and APEC Cross-Border Privacy Rules, alongside national laws such as China's Data Security Law and U.S. cross-border transfer rules. Using qualitative research, comparative legal analysis, and policy review, the study highlights challenges from divergent regulations, ethical concerns over privacy erosion, and compliance burdens for multinational entities. Findings emphasize that reconciling international data mobility with security and privacy requires multilateral cooperation, strong data protection mechanisms, transparency, and independent oversight. Balanced strategies are essential to ensure data flow, safeguard privacy, and mitigate security risks in the digital era.

Keywords:

Data Governance, Privacy Protection, Digital Sovereignty, Regulatory Compliance, International Agreements, Cybersecurity Policy, Personal Information Rights, Transnational Data Transfers

INTRODUCTION

The exponential growth of digital technologies and the global interconnectedness of economies have rendered cross-border data flows indispensable for modern commerce, governance, and innovation. Data, often described as the "new oil," drives critical decision-making processes in sectors ranging from finance and healthcare to artificial intelligence and e-commerce. While international norms encourage the free movement of data to promote efficiency and economic growth, concerns over privacy rights and national security have compelled states to

[1] Advocate Supreme Court of Pakistan. m.atif_iiui@hotmail.com **(corresponding)**

adopt divergent regulatory approaches, creating tension between global interoperability and domestic protection. The purpose of this study is to examine the interplay between international frameworks governing data mobility, national security regulations, and individual privacy rights. It seeks to answer key questions: How can countries reconcile international obligations with domestic security imperatives? What strategies ensure both privacy protection and secure cross-border data flows? The study hypothesizes that multilateral cooperation, data minimization, and transparency mechanisms can mitigate conflicts between privacy rights and national security concerns. Using a qualitative methodology that combines comparative legal analysis and policy review, the research analyses international agreements, national laws, and regulatory practices. Outcomes highlight the ethical, legal, and operational challenges in harmonizing international norms with domestic security needs (Khan & Usman, 2023; Tahir & Tahir, 2024; Kaya & Shahid, 2025).

The article is structured as follows: first, it reviews relevant international frameworks and agreements; second, it examines national security-driven regulations; third, it explores privacy rights and ethical considerations; fourth, it proposes strategies for reconciliation; and finally, it concludes with policy recommendations and directions for future research. In an increasingly interconnected world, data has emerged as a pivotal asset, driving advancements in technology, commerce, and governance. The unrestricted flow of data across borders is essential for the functioning of the global digital economy. However, this openness raises significant concerns regarding the protection of personal information and the potential misuse of data for purposes that may compromise national security. Countries are thus confronted with the challenge of formulating policies that promote the free flow of data while ensuring robust privacy protections and addressing national security risks (Khan, et al., 2023; Mattoo & Meltzer, 2018).

CONCEPTUAL AND THEORETICAL FRAMEWORK

This study is grounded in the intersection of data governance theory, privacy rights frameworks, and national security paradigms to analyze how states regulate and justify cross-border data flows. Conceptually, it draws on the principles of informational self-determination, digital sovereignty, and global data commons to explain competing claims over data control and individual privacy. Theoretically, the research employs a hybrid approach combining liberal internationalism—which supports open data flows through harmonized standards and cooperative regulatory regimes—with securitization theory, which explains how states frame data transfers as national security concerns requiring restrictive measures. By integrating these perspectives, the framework provides a basis for assessing how international norms, domestic legal regimes, and geopolitical interests shape the governance of cross-border data flows and the ongoing effort to balance privacy protection with national security imperatives (Khan, 2025).

RESEARCH METHODOLOGY

This study adopts a qualitative research approach to examine the interplay between cross-border data flows, privacy rights, and national security. The investigation involved a systematic review and comparative analysis of international frameworks, such as the EU–US Data Privacy Framework and APEC Cross-Border Privacy Rules, alongside national laws including China's

Data Security Law and U.S. data transfer regulations. Relevant academic literature, policy reports, government documents, and case law were carefully selected to identify regulatory trends, compliance challenges, and ethical considerations. Data was processed and analyzed thematically to explore the alignment and conflicts between international norms and domestic security measures, assess implications for privacy protection, and evaluate strategies for reconciliation. This methodology was chosen because it allows for a comprehensive understanding of complex legal and policy issues, facilitating evidence-based insights into harmonizing international data governance with national security and privacy imperatives (Kuner, 2010).

INTERNATIONAL NORMS AND FRAMEWORKS

The regulation of cross-border data flows has been shaped by a combination of international agreements, regional initiatives, and voluntary frameworks designed to promote both economic integration and privacy protection. These norms recognize that the free movement of data is critical for global trade, digital innovation, and transnational governance, while also acknowledging the need to protect individuals' personal information. One of the most prominent frameworks is the EU–US Data Privacy Framework, which seeks to facilitate transatlantic data transfers by requiring U.S. companies to adhere to EU-level privacy standards. This framework addresses concerns over U.S. surveillance practices and provides mechanisms for legal redress, ensuring that personal data transferred across borders receives an adequate level of protection. In the Asia-Pacific region, the APEC Cross-Border Privacy Rules (CBPR) System establishes a voluntary set of standards that allow companies to demonstrate compliance with privacy protections while enabling the flow of data across member economies. It promotes accountability, fosters trust between participating organizations, and reduces barriers to international commerce. Other international norms include the OECD Privacy Guidelines, which emphasize transparency, purpose limitation, and security safeguards, and various recommendations by the Council of Europe on data protection in cross-border contexts. These frameworks collectively underscore the recognition that global digital connectivity must be balanced with strong privacy safeguards (KHAN, et al., 2021; Gulia, 2024).

EU–US DATA PRIVACY FRAMEWORK

The EU–US Data Privacy Framework is a key mechanism designed to facilitate the secure transfer of personal data between the European Union and the United States. It emerged as a response to legal challenges surrounding transatlantic data flows, particularly following the invalidation of the previous EU–US Privacy Shield by the European Court of Justice in 2020, which cited insufficient protection against U.S. government surveillance. The framework establishes binding commitments for U.S. companies to comply with EU-level data protection standards, ensuring that personal information of EU citizens is adequately safeguarded when transferred to the U.S. Key provisions include strict limitations on government access to data, independent oversight mechanisms, and the availability of redress channels for affected individuals. The framework also promotes transparency and accountability by requiring companies to implement internal compliance programs, conduct regular assessments, and report breaches or misuse of personal data. By providing a structured legal and regulatory foundation, the EU–US Data Privacy Framework aims to balance the need for seamless cross-border data flows

with the protection of privacy rights. While it enhances trust between organizations and consumers, ongoing monitoring and adjustments are necessary to address emerging technological challenges, evolving privacy concerns, and potential national security conflicts. This agreement aims to facilitate transatlantic data transfers by ensuring that U.S. companies adhere to EU-level privacy standards, addressing concerns over U.S. surveillance practices. (Khan, et al., 2021; Jamil, 2025; Gunasekara, 2009).

Apec Cross Border Privacy Rules System

The APEC Cross-Border Privacy Rules (CBPR) System is a voluntary framework established by the Asia-Pacific Economic Cooperation (APEC) to facilitate the secure transfer of personal data across member economies while ensuring compliance with recognized privacy standards. Introduced in 2011, the CBPR system aims to enhance trust and accountability in the region's digital economy, allowing businesses to demonstrate their commitment to protecting personal information when engaging in cross-border data flows. Under the CBPR system, participating organizations must adhere to core principles, including notice, choice, accountability, and access, which align with globally accepted privacy standards. Companies are subject to independent third-party assessments and certification processes to verify compliance, and enforcement mechanisms are in place to address non-compliance. The system promotes harmonization among diverse national privacy regulations, reducing regulatory fragmentation and lowering compliance costs for multinational businesses. By balancing privacy protection with economic efficiency, the CBPR system fosters a conducive environment for transnational trade and digital innovation. However, its voluntary nature means that participation is limited to willing organizations, and disparities in national regulatory rigor may pose challenges for consistent enforcement and consumer protection across the Asia-Pacific region (Khan, 2024; Singh, 2024).

NATIONAL SECURITY CONCERNS AND REGULATORY RESPONSES

While international frameworks emphasize the free flow of data and privacy protection, national security considerations often drive countries to implement stricter controls over cross-border data transfers. Governments are concerned that personal and sensitive data may be accessed or exploited by foreign entities, cybercriminals, or state actors, potentially undermining national security, critical infrastructure, and public safety. United States: The U.S. has implemented rules restricting data transfers to countries deemed high-risk from a national security perspective, including China and Russia. These measures, particularly under the Department of Justice's 2025 guidance, focus on sensitive government-related data and critical personal information, requiring companies to ensure secure data storage, limit exposure, and report breaches promptly. While these regulations aim to protect national security, they create compliance challenges for multinational companies operating across jurisdictions. China: China's approach emphasizes data sovereignty through its Data Security Law and Personal Information Protection Law, which impose strict requirements on data localization, transfer approvals, and government access. Companies transferring data abroad must demonstrate adequate security measures and obtain regulatory authorization. The laws aim to safeguard both national security and public interest but have raised concerns about the potential for trade barriers and conflicts with international data-sharing norms (Ahmed, et all., 2025; Chin & Zhao, 2022).

Privacy Rights and Ethical Considerations

The protection of privacy rights is a cornerstone of international human rights law and a fundamental ethical obligation in the digital age. Instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights recognize the right to privacy as essential for individual autonomy, dignity, and freedom from arbitrary interference. In the context of cross-border data flows, ensuring privacy protection becomes both a legal and ethical imperative, as personal information may traverse multiple jurisdictions with varying levels of safeguards. Ethical considerations arise when data is collected, processed, or transferred without informed consent, transparency, or adequate protection. The misuse of personal data can lead to surveillance overreach, discrimination, identity theft, and erosion of public trust. Governments and corporations have a responsibility to uphold principles such as data minimization, purpose limitation, accuracy, and security, ensuring that personal information is only used for legitimate purposes and protected against unauthorized access. Balancing privacy rights with national security and commercial interests requires careful attention to necessity and proportionality. Overly restrictive policies may hinder innovation and international commerce, while lax protections risk violating individual rights and ethical norms. Mechanisms such as independent oversight bodies, transparency requirements, and enforceable legal remedies are critical to maintaining accountability and public confidence in data governance frameworks, privacy protection is not merely a regulatory obligation but a moral and societal imperative. Ethical data governance, when integrated with robust legal frameworks, serves as the foundation for trustworthy and sustainable cross-border data flows.The protection of privacy rights is enshrined in various international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Privacy is recognized as a fundamental right, and its erosion can lead to significant ethical and societal implications, such as surveillance overreach and loss of individual autonomy. Balancing privacy rights with national security concerns requires careful consideration of the necessity and proportionality of data protection measures. Overly restrictive policies can stifle innovation and economic growth, while insufficient protections can lead to privacy violations and public distrust (Gul, et al., 2025; Nabiebu et al., 2025).

Reconciling International Norms with National Security

Reconciling the free flow of data, as advocated by international norms, with national security imperatives requires a multifaceted and balanced approach. The challenge lies in ensuring that privacy rights are respected while mitigating risks associated with cyber threats, state surveillance, and sensitive data exposure. Multilateral Agreements: Engaging in multilateral dialogues and treaty frameworks can provide a platform for harmonizing standards across jurisdictions. Agreements like the EU–US Data Privacy Framework demonstrate that structured cooperation can balance privacy protection with cross-border data mobility, creating legal certainty for organizations operating internationally. Data Minimization and Anonymization: Implementing principles of data minimization collecting only necessary information—and anonymization techniques can reduce the risks associated with cross-border transfers. By limiting

identifiable personal data exposure, states and organizations can maintain operational efficiency without compromising security or privacy. Transparency and Accountability Establishing transparent data processing practices and clear accountability mechanisms enhances trust between governments, corporations, and individuals. Reporting obligations, independent audits, and public disclosure of data handling practices strengthen compliance and mitigate potential misuse. Independent Oversight: Creating independent regulatory bodies to monitor data governance ensures that both international standards and national security requirements are upheld. Oversight bodies can mediate conflicts between competing objectives, enforce compliance, and provide remedies for privacy violations. By combining these strategies, countries can achieve a pragmatic balance: facilitating international data flows essential for economic growth and innovation, while protecting citizens' privacy and safeguarding national security interests. The reconciliation of these goals is an evolving process that demands continuous adaptation to technological advances, emerging threats, and shifting legal landscapes (Khan, 2024; Aaronson, 2015).

CONCLUSION

The governance of cross-border data flows sits at the intersection of privacy rights, national security, and international economic integration. This study highlights the tensions between international norms promoting data mobility and domestic regulations aimed at safeguarding sensitive information. Key findings underscore the importance of multilateral cooperation, robust privacy protection mechanisms, transparency, and independent oversight in harmonizing these competing interests. While frameworks such as the EU–US Data Privacy Framework and APEC Cross-Border Privacy Rules provide valuable models for balancing data flow and privacy, national security concerns continue to shape restrictive measures, creating regulatory complexity for multinational organizations. For policymakers, the research emphasizes the necessity of crafting nuanced strategies that enable secure data transfers without undermining privacy or national security. Recommendations include the adoption of standardized compliance protocols, enhanced anonymization and minimization practices, and ongoing dialogue among international stakeholders to address evolving technological and geopolitical challenges. Future research could explore the impact of emerging technologies such as artificial intelligence, blockchain, and quantum computing on cross-border data governance, as well as comparative studies of privacy enforcement mechanisms across jurisdictions. Additionally, empirical research assessing the effectiveness of existing frameworks in mitigating security risks while protecting individual rights would provide actionable insights for law and policy development in the digital age. The intersection of cross-border data flows, privacy rights, and national security is complex and multifaceted. While international norms advocate for the free movement of data, national security considerations necessitate protective measures that can impact these flows. Reconciling these interests requires a nuanced approach that respects privacy rights, addresses security concerns, and promotes international cooperation. Through collaborative efforts and the adoption of balanced policies, it is possible to foster a global digital environment that is secure, trustworthy, and conducive to innovation.The analysis of administrative discretion and judicial review in Pakistan reveals a dynamic yet uneven evolution of legal standards. From the initial reliance on the narrow Wednesbury unreasonableness to the adoption of proportionality and substantive reasonableness, Pakistani courts have progressively sought to ensure that discretionary powers are exercised within

constitutional and legal boundaries. Judicial activism and Public Interest Litigation have further expanded the scope of review, embedding accountability, fairness, and protection of fundamental rights into administrative governance. Despite these advances, several challenges persist. The judiciary continues to grapple with inconsistent doctrinal application, political pressures, and the over-delegation of discretionary powers by legislatures. These factors hinder predictability, weaken the rule of law, and create tension between judicial oversight and executive autonomy. Addressing these challenges is essential for strengthening governance and ensuring citizens' rights are adequately protected. Future reforms should focus on codifying clear standards for reasonableness and proportionality, providing statutory guidance for discretionary powers, and promoting judicial training in balancing executive flexibility with constitutional safeguards. Comparative insights from jurisdictions such as the UK and India suggest that embedding structured frameworks for review can enhance consistency, legitimacy, and public trust.

Further research could explore the integration of international administrative law principles, empirical studies on the impact of judicial review on administrative efficiency, and the role of emerging technologies in shaping administrative decision-making. By emphasizing both accountability and efficiency, Pakistan can develop a judicial review framework that safeguards constitutional values while respecting the practical realities of governance, ensuring that administrative discretion serves public interest in a just and lawful manner. The trajectory of judicial review in Pakistan demonstrates a gradual evolution from deferential Wednesbury unreasonableness to more substantive standards of fairness and proportionality. However, the absence of a settled doctrinal framework continues to create uncertainty in administrative law. For a balanced system, Pakistani courts must articulate clearer tests for reasonableness, emphasizing proportionality and evidence-based decision-making. Simultaneously, legislatures should impose statutory guidelines on discretion, reducing the burden on courts. Future research should explore the integration of international administrative law principles and comparative constitutional jurisprudence to enrich Pakistan's evolving standards of reasonableness.

REFERENCES

Aaronson, S. (2015). Why trade agreements are not setting information free: The lost history and reinvigorated debate over cross-border data flows, human rights, and national security. *World Trade Review*, *14*(4), 671-700.

Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response. *International Journal of Social Sciences Perspectives*, *8*(2), 41-49.

Ahmed, F. A., Gul, S., & Shahzad, S. (2025). ENSURING ACCOUNTABILITY AND TRANSPARENCY IN AI-DRIVEN CORPORATE GOVERNANCE.

Chin, Y. C., & Zhao, J. (2022). Governing cross-border data flows: International trade agreements and their limits. *Laws*, *11*(4), 63.

Gulia, J. (2024). Cross-Border Data Transfers: International Cooperation and Conflicts. *Legal Lock J.*, *4*, 263.

Gunasekara, G. (2009). The "final" privacy frontier? Regulating trans-border data flows. *International Journal of Law and Information Technology*, *17*(2), 147-179.

Hussain, N., Khan, A., & Chandio, L. A. (2023). Legal Safeguards against Mob Justice: An Analysis of Blasphemy Laws in Pakistan and International Human Rights Norms.

Hussain, N., Khan, A., Chandio, L. A., & Oad, S. (2023). Individual criminal responsibility for the crime of aggression: the role of the ICC's Leadership Clause. *Pakistan journal of humanities and social sciences*, *11*(1), 223-232.

Jamil, S. (2025). Cross-Border Data Flow And Privacy: Addressing Global Privacy Challenges In Big Data. *Journal of Big Data Privacy Management*, *3*(01), 41-49.

Kahn, A., & Wu, X. (2020). Impact of digital economy on intellectual property law. *J. Pol. & L.*, *13*, 117.

Kaya, M., & Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. *Interdisciplinary Studies in Society, Law, and Politics*, *4*(2), 219-233.

Khan, A. (2024). The Emergence of the Fourth Industrial Revolution and its Impact on International Trade. *ASR: CMU Journal of Social Sciences and Humanities (2024) Vol*, *11*.

Khan, A. (2024). The intersection of artificial intelligence and international trade laws: Challenges and opportunities. *IIUMLJ*, *32*, 103.

Khan, A. S. I. F., Amjad, S. O. H. A. I. L., & Usman, M. U. H. A. M. M. A. D. (2020). The Evolution of Human Rights Law in the Age of Globalization. *Pakistan journal of law, analysis and wisdom*.

Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, *31*, 393.

Khan, A., & Usman, M. (2023). The effectiveness of international law: a comparative analysis. *International Journal of Contemporary Issues in Social Sciences*, *2*(3), 780-786.

Khan, A., & Usman, M. (2023). The effectiveness of international law: a comparative analysis. *International Journal of Contemporary Issues in Social Sciences*, *2*(3), 780-786.

Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: do information communication and technology (ICT) and economic complexity matter?. *International journal of environmental research and public health*, *19*(19), 12301.

Khan, A., Amjad, S., & Usman, M. (2020). The Role of Customary International Law in Contemporary International Relations. *International Review of Social Sciences*, *8*(08), 259-265.

Khan, A., Bhatti, S. H., & Shah, A. (2021). An overview on individual criminal liability for crime of aggression. *Liberal Arts and Social Sciences International Journal (LASSIJ)*, *5*(1), 432-442.

Khan, A., Hussain, N., & Oad, S. (2023). The Rome Statute: A Critical Review Of The Role Of The Swgca In Defining The Crime Of Aggression. *Pakistan Journal of International Affairs*, *6*(1).

Khan, A., Iqbal, N., & Ahmad, I. (2022). Human Trafficking in Pakistan: A Qualitative Analysis. *Journal of Social Sciences Review*, *2*(3), 257-268.

Khan, A., Javed, K., Khan, A. S., & Rizwi, A. (2022). Aggression and individual criminal responsibility in the perspective of Islamic law.

Khan, A., Jillani, M. A. H. S., Abdelrehim Hammad, A. A., & Soomro, N. E. H. (2021). Plurilateral negotiation of WTO E-commerce in the context of digital economy: Recent issues and developments. *Journal of Law and Political Sciences*.

Khan, A., Usman, M., & Amjad, S. (2020). Enforcing Economic, Social, and Cultural Rights: A Global Imperative. *International Review of Social Sciences (IRSS)*, *8*(09).

KHAN, A., USMAN, M., & RIAZ, N. (2021). The Intersectionality of Human Rights: Addressing Multiple Discrimination. *Asian Social Studies and Applied Research (ASSAR)*, *2*(03), 498-502.

Khan, M. N. I. (2025). Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices.

Kuner, C. (2010). Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, (016).

Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

Nabiebu, M., Ekpo, M. E., & Agube, N. (2025). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits.

Singh, S. (2024). Regulation of Cross-Border Data Flow and Its Privacy in the Digital Era. *NUJS J. Regul. Stud.*, *9*, 38.

Tahir, S., & Tahir, W. (2024). Legal Challenges in Cross-Border Data Transfers: Balancing Security and Privacy in a Globalized World. *Mayo Communication Journal*, *1*(1), 1-11.

Usman, M. U. H. A. M. M. A. D., Khan, A. S. I. F., & Amjad, S. O. H. A. I. L. (2021). State Responsibility and International Law: Bridging the Gap.