ISSN: 2053-3578 I.F. 12.34

THE LEGAL SIGNIFICANCE OF CROSS-BORDER DATA EXCHANGE

Ergashev Xojimurod Ahmadali o'g'li
The university of world economy and
Diplomacy, faculty of international law
Email: xojimurodergashev274@gmail.com

Abstract. In the era of digital globalization, cross-border data exchange has become a central component of international communication, trade, security cooperation, and technological development. However, the rapid intensification of data flows across jurisdictions has revealed significant legal challenges that require harmonized regulation within the framework of information law. This paper analyzes the legal significance of trans-boundary data exchange by examining global standards such as the GDPR, emerging regional regulatory models, and national legislation. It explores key legal dimensions including data sovereignty, privacy protection, cyber security requirements, data localization policies, and the responsibilities of data controllers during international transfers. Special attention is given to the tension between states' desire to maintain control over personal and strategic information and the practical necessity for unrestricted data flow in sectors such as cloud computing, finance, biometrics, telecommunications, and e-commerce. Additionally, the study assesses the impact of inconsistent legal norms across jurisdictions, highlighting the risks of legal fragmentation, compliance burdens, and potential human rights violations related to privacy and informational self-determination. The abstract concludes that strengthening international cooperation, adopting unified technical-legal standards, and enhancing transparency mechanisms are essential for ensuring lawful, secure, and rights-based cross-border data exchange. The findings underscore the importance of developing integrated information law approaches capable of balancing state sovereignty, individual rights, and global digital interoperability.

Key words: Cross-border data; data protection; international law; GDPR; Convention 108+; cyber security; data transfer.

As a result of the rapid development of digital technologies, information has become a key resource of the global economy. Today, trillions of bytes of data are exchanged daily between states, corporations, and individuals. This process has become an essential factor for international trade, financial markets, cloud technologies, artificial intelligence, e-government,

healthcare, and security systems. In particular, cross-border data flows that is, the transfer of data from the territory of one state to the jurisdiction of another have become the foundation of the global digital space. At the same time, the expansion of data flows raises a number of complex issues within the field of information law. First, the growing aspiration of states to ensure "digital sovereignty" strengthening national control over data, preventing the outflow of strategic information, and safeguarding national security may conflict with the requirements of free international data exchange. This tension is clearly reflected in the practices of Uzbekistan, the European Union, the United States, China, and other countries. The protection of personal data, particularly in regions where strict standards such as the GDPR are in force, requires compliance with rigorous conditions for cross-border data transfers. As a result, for international companies, states, and organizations, the process of data exchange has become not only a technical matter but also a complex legal challenge. Second, national legislation concerning data protection, privacy, cybersecurity, protection of state secrets, and data localization differs significantly from one country to another. This creates legal fragmentation, regulatory conflicts, jurisdictional issues, and fundamental questions regarding data ownership and liability in the context of cross-border data exchange. The lack of legal harmonization is particularly risky in sectors such as finance, medical data, biometric information, Big Data, and artificial intelligence systems. Third, the legal regulation of cross-border data transfers is closely linked to a new dimension of human rights the right to informational self-determination. According to this principle, an individual should have the right to determine where, when, how, and by whom their personal data is processed. However, when data crosses state borders, the effective exercise of this right often becomes significantly more complicated. For this reason, cross-border data exchange has become one of the most pressing and complex areas of information law. The system of international legal norms governing cross-border data flows has primarily developed through the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its modernized version, Convention 108+, the European Union's General Data Protection Regulation (GDPR), the OECD Privacy Guidelines, the APEC Cross-Border Privacy Rules (CBPR) system, and United Nations resolutions on information security. All of these instruments seek to regulate cross-border data exchange on the basis of common global principles. Article 4 of Convention 108 establishes the obligation of states to adopt domestic legislation ensuring the protection of human rights in the context of the automatic processing

of personal data.[1] Article 5 requires that data be collected and processed fairly and lawfully, for specified and legitimate purposes, be adequate and not excessive, accurate and up to date, and retained only for a limited period. Article 6 provides that special categories of data including data revealing racial origin, political opinions, religious beliefs, health status, or criminal convictions may be processed only under enhanced protective safeguards.[2] These principles must equally apply in the context of cross-border data transfers. Article 12 of Convention 108 specifically regulates trans-border data flows, stipulating that personal data may be transferred only to states that ensure an adequate level of protection; otherwise, such transfers may result in violations of individual rights.[3] This provision imposes on states the obligation to establish an independent mechanism for assessing the level of data protection in the receiving country. The modernized Convention 108+ introduced even stricter requirements, stipulating that the assessment of the level of protection must take into account not only formal legislation, but also practical implementation, effective safeguards, judicial practice, and the availability of complaint mechanisms for individuals.[4] The GDPR significantly expanded these principles and established one of the strictest and most sophisticated legal mechanisms in the world for regulating cross-border data transfers. Article 44 of the GDPR provides that the transfer of personal data outside the European Union may take place only if all conditions of the transfer ensure guarantees consistent with the protection of fundamental rights.[5] Under Article 45, personal data may be freely transferred, without additional authorization, to countries that the European Commission has recognized as ensuring an "adequate level of protection"; such countries include New Zealand, Japan, South Korea, Canada, and others. If a country does not ensure an adequate level of protection, Article 46 applies, requiring organizations to provide "appropriate safeguards," that is, additional legal guarantees.[6] These safeguards include Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), certification

[1] 108 Convention https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
[2] 108 Convention https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
[3] 108 Convention https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
[4] 108 Convention https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
[5] GDPR https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
[6] GDPR https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

mechanisms, encryption, pseudonymization measures, anonymization, and data segmentation. In particular, Binding Corporate Rules (Article 47) are recognized as a unique international mechanism enabling the free flow of data within multinational corporations, while requiring robust internal audits, monitoring systems, complaint procedures, and external oversight mechanisms.[7] Article 49 provides for derogations, permitting data transfers on the basis of the explicit consent of the data subject, the performance of an international contract, important grounds of public interest, or the establishment, exercise, or defense of legal claims. However, such derogations must not be transformed into regular or systematic transfer practices. One of the key advantages of the GDPR is that it requires the continuation of data protection even after personal data leaves the territory of the European Union that is, the principle of extraterritorial effect applies. The 1980 OECD Privacy Guidelines constitute a soft-law source of global information law. The eight principles enshrined therein Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability form the foundation of modern binding legal systems. In the context of cross-border data flows, these principles promote an approach not of unrestricted data movement, but of responsible and accountable data governance.[8] The APEC Cross-Border Privacy Rules (CBPR) system, in turn, is based on certification mechanisms designed to facilitate data exchange among businesses in the Asia-Pacific region. Under this framework, once a company obtains certification in accordance with established standards, the process of cross-border data transfer between participating economies is simplified. United Nations resolutions on information security in particular Resolutions 68/167 and 71/199 recognize the right to privacy as an inherent human right and call upon states to strengthen international cooperation against cyber-attacks and unlawful surveillance. Taken together, these instruments establish a core global standard aimed at ensuring that cross-border data flows are managed in a secure, lawful, and human rights–compliant manner. These legal mechanisms collectively demonstrate that the primary objective of cross-border data exchange is to ensure the flow of information necessary for the functioning of the global economy, electronic commerce, artificial intelligence, international banking systems, healthcare, and public administration. However, this process must never occur at the expense of the individual's right to privacy, control over personal data, informed consent, or state sovereignty. Therefore, the most

[7] BCR https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en
[8] OECD https://www.oecd.org/en/topics/sub-issues/ai-principles.html

important task facing states today is to strike a balance between data sovereignty and digital integration that is, to support global integration in information exchange while maintaining strict standards for the protection of personal data. These principles have become the central axis of international information law and form the unified legal foundation for governing cross-border data flows. In addition, Schwartz and Peifer (2017), in their article, analyze the central role of cross-border data transfers within the legal system of the European Union, particularly in the process of establishing the European Digital Single Market. The authors provide an in-depth discussion of the legal mechanisms governing the international transfer of personal data.[9] They argue that the European Union's data protection regime particularly the GDPR is generating a global "Brussels Effect" by establishing stringent standards for cross-border data flows, thereby compelling other countries and corporations to adapt to European norms. The article further emphasizes that the mechanisms regulating EU–U.S. data transfers including Safe Harbor, Privacy Shield, and their successor legal arrangements illustrate the complex balance between facilitating international business operations and safeguarding the fundamental right to data protection. According to the authors, although cross-border data exchange is essential for the global economy, it must be reconciled with international obligations to ensure the protection of privacy in democratic societies. For this reason, European law has developed mechanisms such as adequacy decisions, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs). As a result, the article highlights the complex legal interconnections between international trade, state sovereignty, and the protection of personal data as a fundamental right in the context of cross-border data exchange.[10]

In the era of digital globalization, cross-border data flows have become an increasingly vital component of the international economy, public administration, security, and technological integration. However, their legal governance requires a delicate balance between state sovereignty, the right to privacy, and the integrity of the global digital ecosystem. The research demonstrates that although international and regional standards such as Convention

[9] Schwartz va Peifer (2017) https://books.google.co.uz/books?hl=en&lr=&id=k475EAAAQBAJ&oi=fnd&pg=PA253&dq=Schwartz,+P.,+%26+Peifer,+K.+(2017).+%E2%80%9CTransatlantic+Data+Transfers+and+the+European+Dig&ots=Dmg00uKMAx&sig=tW7ARqipIXigGJY3ZsDjT9jHn7s&redir_esc=y#v=onepage&q&f=false

[10] Schwartz va Peifer (2017) https://books.google.co.uz/books?hl=en&lr=&id=k475EAAAQBAJ&oi=fnd&pg=PA253&dq=Schwartz,+P.,+%26+Peifer,+K.+(2017).+%E2%80%9CTransatlantic+Data+Transfers+and+the+European+Dig&ots=Dmg00uKMAx&sig=tW7ARqipIXigGJY3ZsDjT9jHn7s&redir_esc=y#v=onepage&q&f=false

108+, the GDPR, the OECD Privacy Guidelines, and the APEC CBPR system seek to establish uniform safeguards for data transfers, disparities among national legal systems give rise to legal fragmentation, regulatory gaps that threaten the rights of data subjects, and complex compliance obligations for transnational actors. The intersection of global data flows with the constitutionally grounded right to informational self-determination further reinforces the human rights dimension of this issue. Therefore, the article concludes that, in order to establish a stable and legally sound framework for cross-border data exchange, it is essential to expand international cooperation, strengthen harmonized legal standards, and enhance mechanisms of transparency and accountability. Such an approach is capable of ensuring a sustainable balance between state sovereignty, individual control over personal data, and the uninterrupted functioning of the global digital market.

REFERENCES

1. Convention for the protection of individuals with regard to the processing of personal data 108 Convention; https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

2. General Data Protection Regulation; https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

3. Binding Corporate Rules; https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

4. OECD AI principles; https://www.oecd.org/en/topics/sub-issues/ai-principles.html

5. Article; Schwartz and Peifer (2017) “Transatlantic Data Transfers and the European Digital Single Market.”; https://books.google.co.uz/books?hl=en&lr=&id=k475EAAAQBAJ&oi=fnd&pg=PA253&dq=Schwartz,+P.,+%26+Peifer,+K.+(2017).+%E2%80%9CTransatlantic+Data+Transfers+and+the+European+Dig&ots=Dmg00uKMAx&sig=tW7ARqipIXigGJY3ZsDjT9jHn7s&redir_esc=y#v=onepage&q&f=false