MODERN REGULATION OF DATA CIRCULATION IN DEVELOPED COUNTRIES: ORGANISATIONAL AND LEGAL FRAMEWORK

Olefirenko Andriy

DOI: https://doi.org/10.61345/1339-7915.2024.5.14

Annotation. The article was devoted to the study of modern approaches to the regulation of data circulation in developed countries, focusing on the organisational and legal frameworks that ensure secure, ethical, and efficient data governance. It analyzed the principles and mechanisms underlying the legal frameworks, with particular attention to data minimization, transparency, and accountability. Comparative analysis was conducted to explore regional differences in regulatory practices, highlighting the interplay between national priorities and global standards. Special emphasis was placed on understanding how these frameworks have adapted to technological advancements and the increasing complexity of cross-border data flows in the digital economy.

Revealed were the strengths and weaknesses of data regulation practices in regions such as North America, Europe, and the Asia-Pacific. In Europe, the GDPR demonstrated a robust and harmonized approach that influenced global data protection standards, while North America showcased a fragmented landscape with progressive state-level initiatives like the CCPA. In the Asia-Pacific, Japan's Act on the Protection of Personal Information was highlighted for its adaptability and alignment with international norms. These findings underscored the diversity in approaches, shaped by legal traditions, economic contexts, and policy objectives, and their implications for achieving a balanced data governance model.

Substantiated was the necessity of integrating public-private collaborations to address the challenges posed by emerging technologies and dynamic regulatory environments. Examples such as Australia's cybersecurity partnerships and global initiatives like the World Economic Forum's Centre for Cybersecurity highlighted the value of cooperative efforts in ensuring effective regulation. These collaborations provided a blueprint for balancing innovation with regulatory oversight, enabling adaptable and forward-looking governance models capable of responding to rapid technological changes and increasing cyber threats.

Deserves special attention the global influence of the GDPR, which has set a benchmark for transparency, accountability, and consent, inspiring similar frameworks worldwide, including Brazil's LGPD and South Korea's PIPA. The need for continuous updates to legal frameworks, enhanced enforcement mechanisms, and international cooperation was emphasized as critical for addressing enforcement gaps and harmonizing data protection standards. The article concluded with recommendations for further research and policy innovation to strengthen global data governance in the face of ongoing digital transformation.

Key words: data regulation, data flows, legal frameworks, organisational frameworks, General Data Protection Regulation, California Consumer Privacy Act, data privacy, data governance, public-private partnerships, cross-border data flows, data accountability, data minimisation, data transparency, cybersecurity partnerships, global data governance, regional regulatory practices, digital economy, privacy safeguards, information security, technological adaptation.

1. Introduction.

In the contemporary digital age, data has emerged as one of the most valuable resources, driving economic growth, technological innovation, and societal development. With the proliferation of digital platforms, cloud computing, and artificial intelligence, the circulation of data across borders and industries has become a cornerstone of global connectivity and economic integration. However, this rapid expansion of data use presents significant challenges, including concerns over privacy, data security, ethical data use, and regulatory compliance. These challenges underscore the critical need for robust organisational and legal frameworks to govern data circulation.

Developed countries, as leaders in technological innovation and economic powerhouses, have been at the forefront of establishing regulatory frameworks to address these challenges. Legal measures such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States have set benchmarks for global data governance. However, the effectiveness of these regulations, their adaptability to emerging technologies, and their ability to balance innovation with ethical concerns remain subjects of intense debate.

This study is particularly relevant in the context of global digitalization, where harmonized and effective data governance is crucial to managing cross-border data flows, preventing cyber threats, and promoting international cooperation. By exploring the intersection of organisational and legal aspects of data regulation, this research aims to contribute to the ongoing discourse on modernizing data governance in an increasingly interconnected world.

2. The methodological basis of the study was grounded in a comprehensive and multidisciplinary approach, integrating elements of legal analysis, comparative analysis, and a review of best practices in data governance. The study employed a systemic method to examine the organisational and legal frameworks regulating data circulation in developed countries, allowing for a holistic understanding of the principles and mechanisms involved. The research of the following authors also served as a basis: Shanmugam D., Shabanian S., Diaz F., Finck M., Biega A., Ruohonen J., Hjerppe K., Greenleaf G., Erickson, J.

3. The aim of the work is to explore and critically analyze the organisational and legal frameworks regulating data circulation in developed countries.

4. Presentation of the main material.

The organisational framework for data regulation in developed countries involves a network of governmental and independent bodies, each playing a crucial role in ensuring the secure and ethical management of data circulation. National authorities are often at the forefront of regulatory efforts, with agencies such as data protection commissions, cybersecurity agencies, and digital economy ministries assuming central roles. These institutions are tasked with enforcing legislation, monitoring compliance, and providing guidance to stakeholders. For instance, the European Data Protection Board oversees the consistent application of the General Data Protection Regulation across EU member states, ensuring a harmonized approach to data governance [1]. In the United States, the Federal Trade Commission regulates data practices under various consumer protection laws, while sector-specific agencies like the Federal Communications Commission address telecommunications-related data issues [2]. Independent oversight bodies, such as ombudsmen or data protection commissioners, also play a pivotal role in safeguarding individual rights by mediating disputes and investigating breaches.

The role of international organisations further complements national efforts by promoting global standards and fostering collaboration. The Organisation for Economic Co-operation and

Development has established influential guidelines on privacy and transborder data flows, serving as a foundational framework for international policy alignment [3]. The United Nations, through its specialized agencies like the International Telecommunication Union, facilitates global dialogue on data governance and cybersecurity, emphasizing the importance of inclusivity and capacity-building for developing countries. Similarly, the World Intellectual Property Organization addresses the intersection of data protection and intellectual property, particularly in the context of digital innovation. These international entities contribute by harmonizing regulations, reducing conflicts, and ensuring interoperability of frameworks across jurisdictions.

In addition to governmental and international bodies, collaborative models involving public-private partnerships have become integral to effective data regulation. Public-private partnerships leverage the expertise and resources of the private sector while maintaining regulatory oversight to address complex challenges such as cybersecurity threats and cross-border data transfers. For example, initiatives like the Cybersecurity Information Sharing Act in the United States encourage collaboration between federal agencies and private entities to share threat intelligence and improve collective security. In Europe, frameworks such as the Network and Information Systems Directive promote cooperation between public authorities and private operators of essential services to enhance resilience against cyber incidents [4]. Moreover, industry-specific partnerships, such as those in the financial sector, enable the development of tailored regulatory approaches that balance innovation and security. Collaborative platforms, such as the World Economic Forum's Centre for Cybersecurity, provide a space for stakeholders from governments, businesses, and civil society to co-create solutions to emerging data challenges. These partnerships not only foster innovation but also ensure that regulations remain adaptable to rapidly evolving technological landscapes.

Overall, the organisational framework for data regulation in developed countries reflects a multifaceted approach, combining national and international efforts with dynamic public-private collaborations to address the complexities of data governance in a globalized digital economy.

The legal framework regulating data circulation in developed countries is anchored in comprehensive legislation designed to balance privacy rights, data security, and economic interests. The General Data Protection Regulation (GDPR) in the European Union stands as a global benchmark for data protection laws. Enacted in 2018, the GDPR established a harmonized framework across EU member states, emphasizing principles such as data minimization, purpose limitation, and accountability. It introduced stringent requirements for obtaining informed consent, ensuring data portability, and implementing robust security measures. The regulation's extraterritorial scope, applying to entities processing data of EU residents regardless of location, underscores its global impact.

Enforcement mechanisms, including substantial fines for non-compliance, have incentivized businesses worldwide to align with GDPR standards, thereby influencing data protection practices beyond Europe. The California Consumer Privacy Act CCPA, enacted in the United States in 2020, represents a significant legislative effort at the state level to regulate data privacy. The CCPA grants California residents enhanced control over their personal information by providing rights to access, delete, and opt-out of the sale of their data [5]. While the CCPA lacks some of the prescriptive requirements of the GDPR, such as mandatory data protection officers or breach notification timelines, it marks a critical step toward comprehensive privacy legislation in the United States.

The law's emphasis on transparency and consumer rights has set a precedent for other state-level initiatives, prompting discussions on federal data privacy regulation. Other developed nations have implemented legislation tailored to their unique legal and cultural contexts. In Japan, the Act on the Protection of Personal Information serves as the cornerstone of data privacy regulation, incorporating elements of the GDPR while reflecting domestic considerations [6]. The APPI's 2020 amendments expanded its extraterritorial application and strengthened provisions for cross-border data transfers, aligning Japan's framework with international standards.

Australia's Privacy Act 1988, continuously updated to address emerging challenges, outlines principles-based obligations for entities handling personal data, promoting flexibility and adaptability [7]. While these laws share common objectives of protecting privacy and ensuring data security,

differences in their scope, enforcement, and compliance requirements highlight the diversity of regulatory approaches among developed countries.

The principles of regulation governing data circulation in developed countries are foundational to ensuring that data processing activities align with ethical standards, legal requirements, and societal expectations. One of the key principles is data minimization, which mandates that data collected must be adequate, relevant, and limited to what is necessary for the specified purposes. This principle reduces the risk of over-collection and misuse of personal data by requiring organizations to clearly define their objectives and collect only the information essential for achieving them [8]. By limiting the scope of data processing, data minimization helps protect individual privacy and mitigates potential vulnerabilities in data security.

Another fundamental principle is consent, which serves as the cornerstone of lawful data processing. Consent must be freely given, specific, informed, and unambiguous, ensuring that individuals have control over how their personal data is used. Regulatory frameworks such as the GDPR emphasize the importance of clear and affirmative action to demonstrate consent, prohibiting pre-checked boxes or implied agreements. This principle also requires that individuals be informed about the purposes of data processing, the entities involved, and their rights to withdraw consent at any time. Robust consent mechanisms empower individuals while fostering transparency and trust in data-handling practices.

The principle of accountability underscores the responsibility of data controllers and processors to comply with regulatory standards and demonstrate their adherence to these principles. Accountability requires organizations to implement comprehensive data protection policies, conduct regular impact assessments, and maintain records of processing activities. Under the GDPR, accountability extends to appointing Data Protection Officers DPOs for certain entities, ensuring compliance oversight, and providing evidence of compliance during regulatory audits. This principle reinforces the notion that data protection is not merely a technical requirement but a core organizational responsibility.

These principles are complemented by additional regulatory tenets such as purpose limitation, which restricts the use of data to the purposes specified at the time of collection, and integrity and confidentiality, which require organizations to implement security measures to safeguard data from unauthorized access or breaches. Together, these principles create a comprehensive framework that balances individual rights with organizational obligations, fostering a secure and ethical environment for data circulation in the digital economy. By adhering to these principles, regulatory frameworks aim to address the challenges of modern data processing while promoting trust, accountability, and innovation.

Compliance mechanisms are integral to the effective enforcement of data regulation frameworks, ensuring that organizations adhere to prescribed standards and principles. Enforcement mechanisms are primarily administered by regulatory authorities, which are empowered to investigate non-compliance, impose penalties, and mandate corrective actions. For instance, under the General Data Protection Regulation in the European Union, supervisory authorities have wide-ranging powers to conduct inspections, issue warnings, impose temporary or definitive bans on data processing, and levy substantial fines for violations. These mechanisms are designed to deter misconduct, promote accountability, and reinforce the credibility of regulatory frameworks.

Fines serve as a critical compliance tool, providing a financial disincentive for non-compliance. The GDPR, for example, prescribes tiered penalties based on the severity of violations, with fines reaching up to €20 million or 4% of an organization's global annual turnover, whichever is higher. This approach ensures proportionality while emphasizing the gravity of data protection obligations. Similarly, the California Consumer Privacy Act imposes fines for breaches, calculated per violation, which can lead to significant financial repercussions for organizations failing to safeguard consumer data [9]. The transparency surrounding fines and enforcement actions enhances regulatory accountability and raises awareness among stakeholders about the importance of compliance.

Audits represent another fundamental compliance mechanism, enabling authorities to assess whether organizations are meeting their obligations under data protection laws. These audits may be routine

or triggered by complaints, breaches, or other indications of non-compliance. In many jurisdictions, organizations are required to maintain detailed records of processing activities, security measures, and consent management systems to facilitate such assessments. Audits often include evaluating technical safeguards, governance structures, and adherence to principles such as data minimization and purpose limitation. Findings from audits can result in mandatory recommendations, operational changes, or further enforcement actions to address deficiencies.

Regional approaches to data regulation reveal significant variations in legal frameworks, enforcement strategies, and the balance between privacy and innovation. In North America, the regulatory landscape is fragmented, with the United States lacking a comprehensive federal data protection law. Instead, sector-specific laws, such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, govern specific industries. California's Consumer Privacy Act represents a landmark state-level initiative, providing residents with rights to access, delete, and opt-out of the sale of their personal data. However, the absence of uniform national legislation creates challenges in addressing cross-jurisdictional data issues [10]. Canada's Personal Information Protection and Electronic Documents Act provides a unified federal framework that mandates transparency and accountability, although critics highlight its limited enforcement powers and need for modernization.

In Europe, the General Data Protection Regulation sets a global standard for data governance. Its extraterritorial application, strict consent requirements, and robust enforcement mechanisms have established a high benchmark for protecting individual privacy. The GDPR's harmonization across EU member states facilitates cross-border data flows while ensuring consistent safeguards. However, implementation challenges persist, including disparities in enforcement intensity among member states and resource constraints faced by national data protection authorities. Despite these issues, Europe's approach exemplifies the successful integration of legal, organizational, and technological measures to regulate data circulation.

The Asia-Pacific region exhibits diverse regulatory models reflecting varying levels of economic development and cultural priorities. Japan's Act on the Protection of Personal Information aligns closely with international standards, emphasizing data security and cross-border transfer rules. Amendments in 2020 enhanced its extraterritorial reach, underscoring Japan's commitment to harmonizing domestic laws with global practices. Similarly, Australia's Privacy Act 1988, incorporating principles-based regulations, promotes flexibility and innovation. In contrast, countries like China and India adopt stricter, sovereignty-focused approaches. China's Personal Information Protection Law imposes stringent obligations on data localization and government access, reflecting national security priorities. India's proposed Personal Data Protection Bill incorporates progressive elements but faces delays in enactment, revealing governance challenges.

Successful practices highlight the importance of robust regulatory mechanisms. The GDPR's impact extends globally, influencing laws in countries such as Brazil and South Korea [11]. Its principles of transparency, accountability, and consent have become benchmarks for effective data governance. In the Asia-Pacific region, Japan's APPI stands out for its adaptability and alignment with global norms, facilitating cross-border trade while maintaining privacy safeguards. Public-private collaborations, such as Australia's cybersecurity partnerships, demonstrate the value of integrating diverse expertise to address complex regulatory challenges.

Despite successes, challenges and gaps persist across regions. In North America, the lack of federal legislation in the United States creates inconsistencies and compliance complexities for businesses. In Europe, while the GDPR is comprehensive, enforcement disparities and resource limitations undermine its uniform application. In the Asia-Pacific, regulatory diversity and sovereignty-focused approaches hinder regional harmonization, complicating cross-border data flows. Additionally, rapid technological advancements, including artificial intelligence and blockchain, outpace existing regulatory frameworks, necessitating ongoing adaptation to emerging risks.

Addressing these challenges requires enhanced international collaboration, greater resource allocation for enforcement bodies, and continuous legal innovation to align regulatory frameworks with technological realities. By learning from regional strengths and addressing identified gaps, global data governance can evolve to meet the demands of an increasingly interconnected world.

5. Conclusions.

The analysis of modern regulation of data circulation in developed countries underscores the critical importance of comprehensive legal and organizational frameworks to address the complexities of data governance in an increasingly digital world. Robust regulatory mechanisms, such as the GDPR, have set global benchmarks for transparency, accountability, and consent, influencing legislation far beyond their jurisdictions. These frameworks highlight the necessity of harmonizing domestic laws with international standards to facilitate cross-border data flows while safeguarding privacy and ensuring security.

Regional variations in regulatory approaches reflect the diversity of legal traditions and policy priorities. While countries like the United States grapple with fragmented state-level regulations, other nations, such as Japan and Australia, exemplify adaptability through their alignment with global norms and principles. Public-private collaborations have emerged as a critical strategy, enabling the integration of diverse expertise to tackle complex challenges and promote innovation.

However, significant challenges persist, including enforcement disparities, resource limitations, and the rapid pace of technological advancements that outstrip current regulatory frameworks. Addressing these gaps requires enhanced international cooperation, continuous updating of legal provisions, and increased investment in capacity-building for regulatory bodies.

In conclusion, the dynamic landscape of data regulation demands a balanced approach that respects individual rights, fosters economic growth, and ensures the ethical use of data. By learning from successful practices and addressing identified shortcomings, developed countries can lead the way in shaping a secure and equitable global data governance model. Further research and dialogue will be essential to adapt these frameworks to the evolving demands of the digital era.

References:

1. European Data Protection Board. *European Data Protection Board*. Retrieved from: https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en [in English].

   Federal Trade Commission. *Federal Trade Commission*. Retrieved from https://www.ftc.gov/about-ftc/mission [in English].

2. OECD (2002), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris. Retrieved from: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en [in English].

3. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (2016). *Official Journal of the European Union*, L 194, 1–30. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG [in English].

4. Future of Privacy Forum. (2018). *Comparing Privacy Laws: GDPR v. CCPA*. Retrieved from https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [in English].

5. Clifford Chance. (2020, June). *Amendments to the Protection of Personal Information Act of Japan*. Retrieved from https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/06/amendments-to-the-%20protection-of-personal-information-act-of-japan.pdf [in English].

6. Australian Government Office of the Australian Information Commissioner. *Australian Privacy Principles*. Retrieved from https://www.oaic.gov.au/privacy/australian-privacy-principles [in English].

7. Shanmugam, D., Shabanian, S., Diaz, F., Finck, M., & Biega, A. (2021). Learning to limit data collection via scaling laws: A computational interpretation for the legal principle of data minimization. *arXiv*. Retrieved from https://arxiv.org/abs/2107.08096 [in English].

8. Ruohonen, J., & Hjerppe, K. (2020). *The GDPR enforcement fines at a glance*. *Science Direct*. Retrieved from: https://doi.org/10.1016/j.is.2021.101876 [in English].

9. Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, (170), 16-20. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstractid=3836348 [in English].

10. Erickson, J. (2018). *Brazil's General Data Protection Law and GDPR: History, Analysis, and Impacts*. Retrieved from https://www.academia.edu/38941099/Brazils_General_Data_Protection_Law_and_GDPR_history_analysis_and_impacts[in English].

Andriy Olefirenko,
PhD in Law,
doctoral student of the PJSC «Higher Educational Institution
«Interregional Academy of Personnel Management», Kyiv, Ukraine.
E-mail: victor.rovnuy.ta@gmail.com
ORCID: 0009-0005-1400-1172