Research article
UDC 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.15

Legal Issues of Cross-Border Data Transfer in the Era of Digital Government

Gulbakyt Bolatbekkyzy
Wuhan University, Wuhan, China

Keywords

cybersecurity,
data protection,
digital government,
digital technologies,
digitalization,
human rights,
law,
personal data,
privacy,
transboundary exchange

Abstract

Objective: to identify the main legal factors of cross-border data exchange in the context of digital technology proliferation and government digitalization, including legal guarantees, security issues, cybersecurity risks, approaches to regulating and improving the efficiency of data management in various jurisdictions.

Methods: the study relies on synthesis and critical analysis of various aspects of the stated problem, including analysis of primary and secondary sources. By the example of the regulatory policies of China, the US, the EU and EAEU member states, different approaches regarding the restriction or encouragement of free cross-border data transfer are compared. A comprehensive meta-analysis and literature assessment provided insights into the methods used for data protection in different jurisdictions and allowed outlining the framework and directions of the public policy required for effective cross-jurisdictional data transfer.

Results: the main challenges associated with cross-border data transfer in the context of digital technology proliferation and government digitalization, such as growing inequalities in digital development, legal uncertainties, privacy and cybersecurity, etc., were identified. The legal framework of cross-border data transfer in the context of government digitalization and its implementation were analyzed. It contributed to the search for ways to improve the government efficiency in the context of transnational data transfer, including rendering services and promoting openness and public participation.

Scientific novelty: based on the analysis of various jurisdictions' approaches to legal, security and sovereignty issues caused by transnational data transfer, the author reveals the role and applicability of international law, as well as the unique challenges arising in the member states of the Eurasian Economic Union on the way to the formation of transboundary trust space.

Practical significance: the study of these issues may help various public agencies, first of all, governmental and legislative bodies to the elaborate well-targeted political and legal decisions, aimed at achieving a balance between data availability and data security, between the effectiveness of public administration and respect for the human rights. The results obtained will also be of importance for other subjects of relations in cross-border data transfer and regulation of these relations.

For citation

Bolatbekkyzy, G. (2024). Legal Issues of Cross-Border Data Transfer in the Era of Digital Government. *Journal of Digital Technologies and Law, 2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

Contents

Introduction

Transboundary transfer of data in the realm of digital government entails the crossing of national borders with personal or sensitive data for diverse objectives, encompassing the delivery of governmental services, fostering international partnerships, and facilitating data exchange between government agencies and private-sector collaborators. The transfer of data across borders within digital government is essential for enhancing government services and fostering international cooperation. This practice plays a vital role in the advancement of government services and the promotion of global cooperation.

Nevertheless, it presents legal, security, and sovereignty issues that necessitate resolution through international accords and robust data protection measures. Striking a balance between data accessibility and safeguarding is an intricate endeavor, demanding careful navigation by governments while upholding citizens' rights and adhering to international legal frameworks.

Furthermore, currently, there isn't a single globally accepted, harmonized law or regulation regarding transboundary data transmission or comprehensive data regulation that can be unanimously approved by members of the international community. It is worsened by the increasing inequality in proliferation of digital technologies, which are not equally available for all the nations regardless of their GDP.

1. Transboundary data transfer and its role in digital government

1.1. Categorization of transboundary transfer of data

Transboundary transfer of data is divided into four main categories of types, which include: Inter-Governmental (or Government to Government: G2G) data exchange among government agencies from distinct nations, serving objectives like diplomatic collaboration, law enforcement coordination, and disaster response. It is commonly accepted practice when international law enforcement agencies frequently exchange data to combat global crime. For instance, EuroPol facilitates information sharing among European law enforcement agencies to address organized crime and counter terrorism (De Moor & Vermeulen, 2010). In times of international crises, governments collaborate by sharing data to manage disaster response and humanitarian aid efforts. For example, the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) facilitates data sharing during humanitarian emergencies (Bennett, 2002).

Second one is Government to Enterprise (or Government to Business: G2B) Data sharing with private-sector organizations to facilitate public-private cooperation or privatization of government functions (e.g., outsourcing tax administration to private companies). Data pertaining to international trade and customs, including shipping particulars and cargo manifests, are exchanged between governmental entities and

customs authorities to expedite the seamless transit of commodities across international boundaries. In order to prevent firms and people from paying multiple taxes on the same income, tax authorities from several countries may exchange taxpayer information as part of double taxation agreements (Niu et al., 2021).

Then the third one is Government-to-Individual (or Government to Citizen: G2C) Cross-border transfer of citizens' data for international services (e.g., accessing healthcare while overseas). When citizens from one nation travel abroad, their medical records may be accessible internationally to ensure consistent healthcare. For example, the EU's eHealth Digital Service Infrastructure (eHDSI) allows EU citizens to access healthcare data while traveling within the EU (Bruthans & Jiráková, 2023).

Legal frameworks and compliance of transboundary data transfer in digital government play an essential role, which encompasses Data Protection Laws and International Agreements in this regard. If in the first one (Data Protection Laws) data transfers should adhere to the data protection regulations of both the originating and receiving nations, here as an illustration, the European Union's General Data Protection Regulation imposes stringent conditions on transboundary transfer of data, focusing on adequacy determinations, standard contractual clauses, and binding corporate rules, along with that concerning this it would be worth mentioning Chinese Personal Information Protection Law (PIPL), which also has extraterritorial reach and requirements for both government and non-government sectors. Whereas in the second one (International Agreements) certain countries establish bilateral agreements to regulate data transfers. One such agreement was the EU-U.S. Privacy Shield, which facilitated data exchanges between the EU and the United States until it was invalidated in the "Schrems II" case.

Sovereignty concerns along with data localization are gradually becoming one of the most sensitive topics within cross-border data flow. Certain nations enforce data localization mandates, necessitating that specific data categories are kept within their own territory. As an illustration, Russia's data localization regulations dictate that the personal data of Russian citizens must be stored on servers located within Russia (Gurkov, 2021). As another example, just a recent case of Russian branch Yandex.kz in Kazakhstan[1], where Ministry governors and Yandex's representatives came to the agreement to physically relocate its servers to Kazakhstan after the incident of site's block on the territory of Kazakhstan due to the company's unwillingness to abide by the agreement's conditions.

When data is transferred across international borders, security and cybersecurity are equally important. Data must be protected to avoid unwanted access or breaches. In order

[1] Yandex transfers its structure to Kazakhstan under the threat of blocking (August 21, 2023). CNews. https://clck.ru/39o7xf

to guarantee the privacy and security of transferred data, it is essential to use encryption, secure protocols, and strong cybersecurity measures.

Improving government services and promoting international cooperation within digital government requires cross-border data sharing. However, it raises challenges related to sovereignty, security, and law that must be resolved by international agreements and strong data protection protocols. Finding a balance between data accessibility and security is a complex process that requires governments to navigate carefully while respecting the rights of their citizens and following international legal frameworks.

1.2. Data privacy and security concerns in transboundary transfer of data

The data transfer across borders in digital government gives rise to substantial apprehensions regarding data privacy and security. These concerns emanate from various factors, including legal safeguards, security vulnerabilities, cybersecurity risks, jurisdictional complexities, intricate regulations, and the necessity for strong data management. Effectively tackling these concerns mandates the implementation of legal protocols, cybersecurity tactics, and data management procedures aimed at safeguarding the private information of citizens within an ever more interlinked digital realm.

As new advanced technologies continue to evolve, people's expectations for enhanced services and improvements in various aspects of life are on the rise. Technological advancements bring forth better solutions to existing problems while also introducing new concerns related to security and privacy. The digitization of information resources presents increasing challenges to digital data and infrastructure. While advanced nations have rigorously tested security measures and optimization techniques, developing countries still face inadequacies in addressing these issues[2].

Transboundary transfer of data involves adhering to legal bases and regulatory requirements that are essential for the unobstructed movement of data. These requirements apply to both internal transfers within an organization that extends across national boundaries and external transfers to organizations in different countries. For instance, many jurisdictions, including the EU, UK and China have established regulations stipulating that to ensure the safe and lawful transfer of data from one country to another, the recipient country must uphold privacy standards for personal information that are at least on par with those of the sending country. Only when this equivalency is verified can an adequacy decision be granted by a data privacy regulatory

[2] UNGA. Nearly Half of the World's Population is Excluded from 'Benefits of Digitalization', the Speaker stresses as the Second Committee Debates Information Technology for Development. https://clck.ru/39o86M

body or government authority (in the EU case it is conducted by the European Commission), allowing for the unrestricted flow of data across borders.

2. Securing and enhancing transboundary transfer of data

2.1. Security mechanisms in the transboundary transfer of data

In order to comprehensively cover the current environment of security in the cross-border data-transfer, this chapter, examines the practices of various range in place. Despite the fact that there is no worldwide framework for certifying data protection adequacy to enable transboundary transfer of data, nevertheless, numerous countries and regional groups have implemented their own rules and regulations to oversee these data transfers across borders. For transboundary transfer of data there are five widely used mechanisms that are in place:

1. Decisions on adequacy: Some data protection rules allow data to be transferred to areas recognized by a public body as having data protection standards that are on par with or higher than those of the home country. The European Commission, under the EU's General Data Protection Regulation, is responsible for issuing adequacy determinations. Research conducted by the IAPP reveals that 74 jurisdictions authorize public entities, such as data privacy regulators or government authorities, to issue adequacy determinations for data transfers[3]. It's critical to understand that adequacy rulings are not always final and could be reevaluated in response to changing circumstances or modifications to data protection laws.

2. Contractual agreements: or data transfer contracts are employed to authorize data transfers beyond the boundaries of an organization's jurisdiction. These contracts guarantee the strict observance of pertinent compliance standards, such as those pertaining to data processing and storage. Standard Contractual Clauses (SCCs) are the most commonly used contractual clauses in practice. These are pre-written clauses that can be included into contracts between data importers and exporters for transboundary transfer of data. The European Commission has approved them as complying with the GDPR. 71 countries presently have drafts, templates, or standardized contractual clauses available, according to the IAPP's evaluation[4].

3. Intra-organization transfers or Binding Corporate Rules (BCRs) represent a collection of internal policies and agreements that govern data compliance and authorize transboundary transfer of data within a single organization. The recognition of BCRs extends to various jurisdictions, including the EU, UK, Brazil, Singapore, and South Africa. Many organizations opt to adopt EU BCRs to structure their global data privacy compliance initiatives. However,

---

3 International Association of Privacy Professionals. Infographic: Global Adequacy Capabilities. https://clck.ru/39o88u

4 Ibid.

implementing BCRs can be an intricate and time-consuming process, as it necessitates approval from pertinent data protection authorities.

4. Certification mechanisms: Several jurisdictions acknowledge certifications issued by approved data authorities for transboundary transfer of data. To achieve certification, businesses must secure approval from an independent Accountability Agent (AA). These AAs can be either public entities or private organizations. Presently, the sole certification-based transfer mechanism in use is the APEC Cross-Border Privacy Rules (CBPR) System. This certification validates compliance and holds recognition in eight countries: Australia, Canada, China, Japan, South Korea, Mexico, Singapore, and the US.

5. User consent: While challenging to scale, securing user consent has traditionally been the primary approach for transboundary transfer of data, especially in complex legal environments where consent is the central element amidst various data transfer frameworks. User consent must meet specific criteria, including being informed, explicit, and unambiguous, with standards for obtaining consent varying across jurisdictions. Under the GDPR, user consent may serve as a transfer mechanism only when no adequacy decision or suitable safeguards, such as SCCs or BCRs, are available. The lack of a global framework for the certification of adequate data protection can make it challenging for organizations to navigate the complex landscape of data protection regulations.

In this regard numerous governments are actively addressing the challenge of transboundary transfer of data. They are collaboratively striving to create a favorable setting for legitimate cross-border data flows, all the while safeguarding individual privacy rights and upholding data security.

2.2. Governments' initiatives enhancing the efficiency of transboundary transfer of data

Here are some recent initiatives undertaken by particular governments to enhance the efficiency of transboundary transfer of data.

The European Union and United States have collaboratively introduced a new EU-U.S. Data Privacy Framework (DPF)[5]. This framework replaces the former Privacy Shield framework, which was invalidated by the Schrems II ruling in 2020. The European Commission has been instructed not to approve the framework until it has been updated to adequately address the concerns expressed by the Schrems II case by both the EU Parliament and the EU Data Protection Board (Gao & Chen, 2022).

Under the leadership of Japan, G7 governments are actively developing the Institutional Arrangement for Partnership (IAP)[6]. This partnership aims to bridge the gap in creating

[5] International Association of Privacy Professionals. (n.d.). EU-U.S. Data Privacy Framework: Guidance and Resources. https://clck.ru/39o8Dg

[6] World Economic Forum. (2023, April 26). How and why data must flow freely and responsibly across borders. https://clck.ru/39o8Gf

an effective and trusted international cooperation mechanism for operationalizing Data Free Flow with Trust (DFFT).

As of June 1, 2023, China implemented the Measures on the Standard Contract for the Transboundary Transfer of Personal Information. These measures mandate that specific personal data processors, even those handling data for fewer than 1 million individuals, must enter into contracts with overseas recipients before transmitting data abroad. China's overarching legislative framework for managing data security encompasses three key laws: the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. These laws are supported by a range of governmental regulations that are consistent with the legal framework. Under these laws, the central government has established its regulatory system for the export of personal data.

Additionally, a Global Cross-Border Privacy Rules (CBPR) forum has been established (Joel, 2023). Member economies of the Asia-Pacific Economic Cooperation (APEC), including the United States, Canada, Japan, Singapore, and others, have initiated this forum with the objective of setting up an international certification system based on the APEC CBPR System and related Privacy Recognition for Processors (PRP) Systems.

As the digital economy undergoes rapid transformation, organizations must remain agile and proactively update their methods and protocols to align with the ever-changing regulatory environment. This is particularly crucial for large organizations with extensive global operations, as non-compliance can result in substantial fines. In 2021, for instance, European data protection supervisory authorities imposed fines amounting to nearly $1.2 billion USD, with the largest fine levied against a US-based online retailer[7]. Chinese companies based within the country, aiming for international initial public offerings, continue to grapple with the repercussions of the China's Cyberspace Administration (CAC) fining the prominent ride-hailing firm, Didi Global, a substantial 8 billion yuan ($1.2 billion) last year for violations of national security and personal information protection regulations[8].

Given the various mechanisms available for facilitating transboundary transfer of data, it is incumbent upon each organization to evaluate and choose the most suitable options based on their specific needs. There is no one-size-fits-all solution. Depending on the use cases, governments may discover the need to employ multiple frameworks to address their particular requirements. It is also vital to consider how the data transfer approval process can be seamlessly integrated into existing workflows. Failure to establish an efficient and appropriate process can result in prolonged and costly endeavors when seeking clearance for data transfers on an ad-hoc basis.

---

7 EDPB. (2023, May 22). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. https://clck.ru/39o8HK

8 Webster, G. (2022, July 21). Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. DigiChina. https://clck.ru/39o8KA

3. The relevance of international law in regulating transboundary transfer of data

3.1. Different approaches of jurisdictions on transboundary transfer of data

Needless to say, that the role of international law in the regulation of transboundary transfer of data is quite crucial, serving as a cornerstone for safeguarding privacy, upholding human rights, ensuring cybersecurity, facilitating trade, resolving conflicts, and establishing customized agreements. It lays the groundwork and outlines the standards for the appropriate management of data across international borders, promoting responsible data governance and nurturing confidence in digital interactions.

It was noted that the internet "cannot be regulated". The nation-state is irrelevant, not laws; that is the difference (Chuanying, 2020). A joint study commissioned for the Defense Department in 1998 observed:

It may be that the real problem created for governments by the proliferation of the Internet (and other IT-enhanced communications media) is not the proliferation of information so much as the proliferation of actors on the governmental and diplomatic stages. Organized groups and individuals can build, and in fact are building, coalitions, both domestic and international, that can bring unprecedented pressure to bear on national governments regarding virtually any activity or area of interest. These groups may in fact create faits accomplish that require no more action of governments than to accept what has already been accomplished. This raises the question of whether the nature of sovereignty has changed in the area of instant and ubiquitous communications and, if so, how (Press et al., 1998).

An associate professor at the University of Maryland, College Park Dr. Virginia Haufler disagrees, stating, "The decentralized, open, global character of... the Internet makes it difficult to design and implement effective regulations through top-down, government-by-government approaches" (Haufler, 2013).

The devastating circumstances of the 9/11 terrorist attacks and the terrorists' use of the Internet for communication accelerated the developed world's adoption of content restriction. According to an advocacy group that backed journalistic freedom, as early as September 2002, the United States, the United Kingdom, France, Germany, Spain, Italy, Denmark, the European Parliament, the Council of Europe, and the G8 countries had all expressed worries about their rights and freedoms online (Nijboer, 2004).

International governmental organizations have faced significant challenges as a result of substantial differences in state objectives for content restriction. During the inaugural session of the World Summit for the Information Society (WSIS) in December 2003, this division was made evident. The wording employed to address the consequences of any agreement on the management of Internet speech was one of the key areas of contention during the WSIS negotiations. China, not insignificantly, voiced its disapproval of the press freedom text that reflected American influence. As a result, the Declaration of Principles did mention press freedom, but it did so in a way that was more subdued and added language

emphasizing the integration of national sovereignty[9] (Berleur, 2007). Governments were required by the Action Plan to take necessary measures to address harmful and illegal media content while upholding the right to free speech (Jensen, 2006). External observers agreed that the plan of action covered up irreconcilable disagreements on content regulation and provided little guidance for the future (Souter, 2004).

As an example, the United States and the European Union have different approaches to data privacy. The American position on private rights is based mostly on the notion of non-interference from the government. As a result, there hasn't been much support in the US for extensive state laws pertaining to data privacy. Bessette and Haufler (2001) have observed that the US prefers a more market-driven method of data collection. "If private sector privacy protections can be adopted internationally, that would naturally become the prevailing method for safeguarding privacy", stated Ira Magaziner, one of the representatives of President Administration (Farrell, 2003).

In contrast, privacy is regarded in Europe as a fundamental right that needs to be safeguarded by the government. Bessette and Haufler point out that "European nations, in particular, have put in place robust privacy safeguards, defining privacy as a fundamental human right" as a result of past instances of privacy infringements by the government (Mai'a, 2023). The European Union passed the comprehensive Data Protection Directive in 1995, giving European businesses clear regulations and enforcement mechanisms. This directive was designed to prevent companies from operating outside of EU jurisdiction in order to evade the law. It prohibited the transfer of personal data belonging to EU citizens to nations that did not offer adequate security. In late 1998, the directive was scheduled to go into force (Long & Quek, 2002).

In view of the extent to which this prohibition was, nations like Australia, Canada, and Eastern Europe were compelled to change their own legal systems to comply with EU standards. Nevertheless, the US retaliated by pressuring US multinational corporations to establish self-regulatory frameworks compliant with EU laws.

Totalitarian regimes have employed straightforward yet efficient methods for regulating Internet content. There were cases of restricting use of personal computers, controlling and prohibiting objectionable content (in regards of pornographic materials; immoral websites; religious and politically sensitive content) which eventually led to the Internet censorship using filtering system extensively (Drezner, 2004).

Scholars studying globalization have frequently oversimplified the intricate web of governance interactions in international politics by focusing exclusively on the binary opposition between state and nonstate power. A more perceptive view of the effects

[9] McCarthy, K. (2003, December 8). Internet Showdown Side-stepped in Geneva. The Register Newsletter, 8. https://clck.ru/39o8LW

of globalization is offered by acknowledging the possibility of diverse global governance arrangements. An examination of Internet governance shows that governments may nevertheless intervene when necessary to further their own goals, even if they choose to assign governance duties to commercial organizations.

Whenever major powers are unable to cooperate, but other international players support no less than one of the main nations, the result is commonly referred to as "rival standards". Two instances of such rival standards were identified in the case studies: data privacy and regulations for genetically modified organisms (Trump et al., 2023). In both of these cases, the USA and the EU have each propagated distinct sets of rules for regulating these matters. Both parties have managed to secure some level of support, yet neither standard has achieved universal acceptance.

Lastly, it is projected that if the major powers concur but their interests do not align with those of other international actors, the outcome will be "club standards". These standards represent one of the most captivating facets of regulatory processes. In this scenario, the influence of major powers is readily apparent as they exert pressure on and negotiate with other states to establish a standard. This often begins with a small yet influential group, such as the OECD or the Financial Action Task Force on Money Laundering. These coalitions of like-minded states have the capacity to formulate regulations and subsequently persuade or persuade other states to conform to them.

3.2. The privacy shield of the EU-US and its impact on transboundary transfer of data between the EU and the US

The U.S.-EU Privacy Shield was a framework designed to regulate the transfer of personal data from the European Union to the United States. Ensuring that these data transfers followed European data protection regulations was its main goal. After the ECJ overturned the Safe Harbor framework in the wake of the 2015 "Schrems I" decision, this new structure was implemented in 2016. Establishing a legal framework for the transfer of EU personal information to the US and making sure US organizations upheld data protection standards comparable to those in the EU was its main goal.

The European Commission determined that the Privacy Shield offered a suitable level of data protection in the US, and as a result, the EU data protection framework awarded it an "adequacy decision". All pertinent facets of a data transfer operation, or series of related acts, were to be taken into account when determining the protection level. Many variables were considered in this review, including "the legal regulations, both overarching and specific to the third country involved, as well as the professional standards and security measures followed in that country" (Hijmans, 2006).

In order to prevent companies from processing data outside of the EU for the purpose to obtain an exemption from the 1995 Directive, the transfer limitation was implemented

(Drezner, 2008). Some nations did change their laws in an effort to achieve adequacy standards as a result of this clause. But rather than supporting enforceable legislative measures, the United States supported self-regulatory options that were consistent with the federal data privacy policy's self-regulatory nature (Voss, 2019).

Numerous studies have contrasted US and EU approaches to internet regulation policymaking. The results show that the EU generally produces broad and comprehensive legislation. But this legislative procedure frequently moves more slowly, which can be problematic, especially when dealing with the internet's rapid evolution and emerging technology. The US, on the other hand, has a more decentralized regulatory framework with multiple agencies and occasionally incompatible regulations (Reidenberg, 1996).

The substantial disagreement between the two stems from differences, further exacerbated by distinctions between data and metadata. US federal law grants law enforcement significant authority to access metadata (Schneider, 2009).

But with regard to the Privacy Shield, the European Commission's Decision No. 2016/1250 was declared illegal by the CJEU. This resulted from the decision's failure to guarantee a degree of personal data protection equivalent to that required by European legislation (Furramani, 2023).

2016 marked the establishment of European Commission Decision No. 2016/1250, which allowed the transfer of personal data from the EU to the US. This framework was used by EU and EEA businesses to send personal data to US entities listed under the Privacy Shield, offering specific safeguards for data protection (Furramani, 2023).

The case concerned a Facebook[10] user who was an Austrian national and disputed that his data have been transferred to the US because the US did not offer the same level of protection as required by EU legislation. This disagreement resulted in a 2013 complaint that the Data Protection Commissioner initially took an examination at.[11] After reevaluating, the Commissioner concluded that the transfer of personal data to the United States did not comply with Articles 7, 8, and 47 of the European Charter of Fundamental Rights[12]. This prompted the case to move to the High Court.

According to the High Court, the US did not ensure adequate protection for personal information in line with EU Charter of Fundamental Rights Articles 7 and 8. The Court identified several issues, including the application of the Fourth Amendment to European nationals, concerns about the National Security Agency's activities without judicial oversight,

[10] A social network blocked in the territory of the Russian Federation for disseminating illegal information.

[11] CJEU, Schrems II, 2020, July 16, paras 50, 51 and 52.

[12] CJEU, Schrems II, 2020, July 16, paras 55 and 56.

and the Privacy Shield's Ombudsperson not meeting Article 47 of the Charter. In light of these matters, the High Court referred the case to the CJEU[13].

As stated in Article 45 of the GDPR, the CJEU's decision established that transfers of personal information from the EU or EEA to a third country must be predicated on an adequate decision made by the Commission. If such a decision is not made, data may be transferred in accordance with Article 46 of the GDPR's "appropriate safeguards", which guarantee subject rights and legal remedies[14].

The Court highlights the importance of national supervisory bodies with respect to protecting personal information, in line with GDPR Articles 51(1) and 57(1). It highlights that national authorities are in charge of ensuring that the norms specified in EU regulations are adhered to when personal data is transferred from the EU or European Economic Area (EEA) to other nations or international organizations[15] [16].

National supervisory authorities should be able to look into complaints and assess if transferred data conforms with GDPR rules even in situations where the European Commission has approved an adequacy judgment allowing the transfer of personal information[17] [18].

According to the CJEU, the Privacy Shield does not guarantee data subjects' rights that are enforceable and effective in the face of interference, as stated in the European Union's Charter of Fundamental Rights. The right to a fair trial and an effective remedy are guaranteed by this charter. Furthermore, the CJEU determined that, in accordance with Article 47 of the Charter, the Secretary of State's designated Privacy Shield ombudsperson is neither an autonomous entity nor a tribunal[19].

The CJEU concluded, in essence, that the USA does not offer a level of data protection that is effectively comparable to that of the European Union, as required by Article 45(1) of the GDPR, taking into account Articles 7, 8, and 47 of the Charter. These articles guarantee the right to efficient legal protection, respect for one's privacy and family life, and protection of one's personal data. As a result, the sufficiency ruling was overturned. In light of this, data transfers between the US and the EU must rely on extra precautions specified in EU Regulation Chapter V, namely Article 46(2), which outlines appropriate safeguards.

On June 4, 2021, the European Commission approved two sets of standard contractual agreements in reaction to the withdrawal of the Privacy Shield[20]. The purpose of these regulations is to make it easier for personal data to be transferred from the EU to third

13 CJEU, Schrems II, 2020, July 16, para. 65.

14 CJEU, Schrems II, 2020, July 16, paras. 91 and 92.

15 CJEU, Schrems II, 2020, July 16, para. 107 and case C-362/14, 2015, October 6, Schrems I, para. 47.

16 This perspective aligns with the Court's reasoning in the Schrems II case of 2020 and the Schrems I case of 2015, as well as insights presented by scholars such as Piroddi in 2021 and De Mozzi in 2022.

17 CJEU, Schrems II, 2020, July 16, para. 120.

18 This principle was upheld in the Schrems II case of 2020.

19 CJEU, Schrems II, 2020, July 16, para. 168.

20 Commission implementing decision of 4 June, Nos. 2021/914/UE and No. 2021/915/UE.

countries. These commercial agreements cover the requirements for personal data transfers in compliance with the ECJ's Schrems II case judgment, as well as provisions to accommodate the variable number of parties adhering to the contract (De Mozzi, 2021).

3.3. Transboundary transfer of data within the Eurasian economic union

Digital technologies present novel opportunities for customs authorities to enhance both the speed and quality of their decision-making processes. The next phase in advancing digital government administration is closely linked to data centralization. This involves structuring public governance, where decisions increasingly rely on objective data (Vovchenko et al., 2019).

Creating a common platform for digital data exchange and transmission is another essential component in digitizing the customs regulatory system in the EAEU, which is highlighted in its Cross-Border E-Trust Space along with the treaty of the organizations, particularly in its Art. 23.

Additionally, the Eurasian Economic Commission has laid the groundwork for a transnational takeover of the digital economy. This was made possible by the October 11, 2017, Supreme Eurasian Economic Council No. 12 decision, which approved the primary plans for implementing the digital agenda of the EAEU through 2025 (Kolodnyaya, 2018).

Even though the bulk of the aforementioned laws were passed within the EAEU, there are still a number of barriers that make a smoother transition for all of the union's members more challenging. The persistent problem, remaining as a major obstacle of regulating data circulation throughout the Union is a significant barrier to the implementation of the digital agenda. Many digital ecosystems planned for implementation involve cross-border data exchange in various interaction formats, including G2G, G2C, G2B, B2B, and B2C. However, numerous aspects of data circulation in the EAEU remain underdeveloped. Consequently, there is a lack of terminological consistency in key concepts related to data, and the regulation in the category of data is inadequately developed, lacking common approaches to the legal categorization of data and risk management in this domain. Legal matters stemming from cross-border data exchange have yet to be addressed. As a result, regulatory measures are lagging behind practical considerations, impeding progress in the digital agenda. The situation is further complicated by requirements outlined in the national legislations of EAEU Member States, particularly those concerning the localization of personal data. As a result, it is crucial to create and enact legislation as well as an appropriate data protection mechanism for cross-border data circulation inside the EAEU, comprising both non-personal and personal data (Mikhaliova, 2022).

The Union has been engaged in prolonged discussions regarding the development of an international agreement concerning data circulation and data protection. However, the process of aligning approaches and crafting such an agreement continues to be intricate and time-consuming.

Moreover, challenges in the realm of electronic document management persist. Consequently, there is a need for legislative enhancements and the formulation of shared

approaches in the domain of electronic signatures. The issue of mutually recognizing electronic signatures stands out as a prominent barrier to seamless trade, significantly complicating interactions with suppliers in the internal market of the EAEU and the procurement process. The effective utilization of the Union's digital infrastructure remains unattainable without the resolution of these legal gaps.

A more intricate obstacle to the realization of the digital agenda pertains to the issue of unequal digital advancement among the Member States of the Union (Filatova et al., 2018). To demonstrate this challenge, we can examine the performance of these Member States within the Networked Readiness Index.[21]

The World Economic Forum created the Networked Readiness Index in 2002 and now administered by the Portulans Institute and provides a measure of the degree of information and communication technology development in different nations. This index assumes a pivotal role in assessing a nation's technological and innovative capabilities and provides a valuable means for conducting comparative evaluations of ICT progress across states.

Concerning information and communication technology advancement within the EAEU region, there is a noticeable disparity. For example, in 2022, the ICT development gap between Russia and Kyrgyzstan was a substantial 45 points. Armenia, Belarus, and Kazakhstan have reached comparable levels of ICT development, but their disparities with Russia are also considerable. Currently, the focus is on enhancing the connectivity of government bodies in EAEU Member States, updating the integrated information system, and implementing secure and continuous electronic document management, which has mitigated this issue to some extent.

However, in the future, as the Union's digital initiatives directly impact the interests of the population, this digital divide could significantly impede the efficiency of project implementation. Additionally, the current digital initiatives rely on the pre-existing national services, and the varying levels of development in these services complicate the execution of collaborative projects (Bolgov & Karachay, 2016). To expedite the digital transformation of the Member States, it is imperative to intensify the international exchange of digital technology expertise and the expansion of best technological practices.

Crucially, the internal digital infrastructure of the Union, notably the integrated information system, has yet to be fully established. Additionally, the execution of several pivotal projects within the digital agenda is experiencing delays. The primary hindrances impeding the advancement of the Union's digital ecosystem include deficiencies in the legal framework, a lack of coherent conceptual alignment in the implementation of national digital economy strategies, and disparities in ICT development across the region.

In recent years, the EAEU-states have been actively establishing their respective national digital ecosystems. These efforts have spanned both the realm of public administration and the advancement of digital economies within their own borders. However, the progress

21 Network Readiness Index Homepage. https://networkreadinessindex.org

of the EAEU's digital agenda has not kept pace with the development of national digital ecosystems. The initial delays have created challenges in harmonizing collective approaches and strategies, ultimately resulting in a decrease in the number of proposed digital initiatives.

To effectively realize the goals and objectives outlined in the digital agenda, it is imperative to consolidate the endeavors of EAEU-states in the field of digital economic transformation. This consolidation should involve a more robust engagement of national competence centers and the enhancement of national digital infrastructures.

Conclusion

It is obvious, that currently the international community more than ever needs a regulatory coordination framework, which concerns transboundary transfer of data that come along with legal safeguards and can highlight security vulnerabilities, cybersecurity risks and jurisdictional complexities.

Harmonized standards are established when there is significant agreement between major countries, major powers and other international entities. Instead of being managed by local or exclusive organizations, these norms are expected to form a vast "regime complex" that is overseen by "universal" intergovernmental organizations. One good example of harmonized standards, as it was mentioned earlier, is the widespread use of the TCP/IP Internet protocol.

References

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference "Information Society: Governance, Ethics and Social Consequences", University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union's countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects

and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Kolodnyaya, G. (2018). Digital economy: features of development in Russia. Ekonomist, 4, 63–69. (In Russ.).

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Author information

Gulbakyt Bolatbekkyzy – PhD Candidate and Doctoral Scholar, School of Law, Wuhan University
Address: Luojia Hill, Wuhan, Hubei Province, 430072, China
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313-2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 2, 2024
Date of approval – March 1, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.15

Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления

Гульбакыт Болатбеккызы

Уханьский университет, Ухань, Китай

Ключевые слова

государственное управление,
защита данных,
кибербезопасность,
конфиденциальность,
персональные данные,
права человека,
право,
трансграничность,
цифровизация,
цифровые технологии

Аннотация

Цель: определить основные юридические факторы трансграничного обмена данными в контексте распространения цифровых технологий и цифровизации государственного управления, включая правовые гарантии, проблемы безопасности, риски кибербезопасности, подходы к регулированию и повышению эффективности управления данными в разных юрисдикциях.

Методы: исследование опирается на синтез и критический анализ различных аспектов заявленной проблемы, в том числе на анализ как первичных, так и вторичных источников. На примере сравнения политики регулирования Китая, США, ЕС и государств-членов ЕАЭС сопоставляются различные подходы относительно ограничения или поощрения свободной трансграничной передачи данных. Комплексный мета-анализ и оценка литературы позволили сформировать представление о методах, используемых для защиты данных в разных юрисдикциях, а также обозначить рамки и направления государственной политики, необходимые для эффективной передачи данных между юрисдикциями.

Результаты: выявлены основные проблемы, связанные с трансграничной передачей данных в контексте распространения цифровых технологий и цифровизации управления, такие как растущее неравенство в развитии цифровых технологий, правовая неопределенность, обеспечение конфиденциальности и кибербезопасности и др. Проанализированы правовые основы трансграничной передачи данных в контексте цифровизации государственного управления и практика их реализации, что способствовало поиску путей повышения эффективности управления в условиях транснациональной передачи данных, включая предоставление услуг, развитие открытости и участия общественности.

Научная новизна: на основе проведенного анализа подходов различных юрисдикций к проблемам юридического характера, вопросам обеспечения безопасности и суверенитета, обусловленным трансграничной передачей данных, выявлены роль и применимость международного права, а также уникальные вызовы, возникающие в государствах-членах Евразийского экономического союза на пути формирования трансграничного пространства доверия.

Практическая значимость: исследование указанных вопросов имеет значение для выработки и принятия взвешенных политико-правовых решений государственными структурами, прежде всего правительственными и законодательными органами, направленных на достижение баланса между доступностью данных и их безопасностью, между эффективностью государственного управления и соблюдением прав граждан. Полученные результаты будут иметь значение также для иных субъектов отношений, связанных с трансграничной передачей данных и вопросами регулирования указанных отношений.

Для цитирования

Болатбеккызы, Г. (2024). Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления. *Journal of Digital Technologies and Law*, *2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

Список литературы

Колодняя Г. (2018). Цифровая экономика: особенности развития в России. *Экономист*, *4*, 63–69.

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference "Information Society: Governance, Ethics and Social Consequences", University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union's countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Информация об авторе

Болатбеккызы Гульбакыт – соискатель степени PhD, докторант, школа права, Уханьский университет
Адрес: 430072, Китай, провинция Хубэй, г. Ухань, Луоцзя Хилл
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313–2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 2 февраля 2024 г.
Дата одобрения после рецензирования – 1 марта 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.