UZBEK LAW REVIEW

VOLUME 1
2025

ЎЗБЕКИСТОН ҚОНУНЧИЛИГИ ТАҲЛИЛИ

UZBEKISTAN LAW REVIEW

ОБЗОР ЗАКОНОДАТЕЛЬСТВА УЗБЕКИСТАНА

ИЛМИЙ ТАҲЛИЛИЙ ЖУРНАЛ	SCIENTIFIC ANALYTICAL JOURNAL	НАУЧНО АНАЛИТИЧЕСКИЙ ЖУРНАЛ

2025

№1

Маълумот олиш учун қуйидагиларга мурожаат этиш сўралади:
Гулямов Саид Саидахрарович,
Рустамбеков Исламбек Рустамбекович
ТДЮУ, Халқаро хусусий ҳуқуқ кафедраси,
Ўзбекистон Республикаси, Тошкент ш., 100047,
Сайилгоҳ кўчаси, 35. Тел: 233-66-36

"Ўзбекистон қонунчилиги таҳлили"нинг электрон нусхаси Интернетдаги www.library-tsul.uz ёки www.lawreview.uz сайтида жойлаштирилган.

Журнал 2013 йилдан Ўзбекистон Республикаси Вазирлар Маҳкамасининг Олий Аттестация комиссияси журналлари рўйхатига киритилган.

2025 йилда нашр этилди.

ISSN 2181-8118

Масъул котиб: **И. Рустамбеков**
Нашриёт муҳаррири: **Н. Ниязова**
Техник муҳаррир: **Д. Козимов**
Лицензия № 02-0074
Босишга рухсат этилди – 28.03.2025
Нашриёт ҳисоб табоғи – 5
«IMPRESS MEDIA» босмахонасида босилди
Адади – 100 нусха.

ИЛМИЙ-ТАҲЛИЛИЙ ЖУРНАЛ

1/2025

Wang Cong
Doctoral Student at the University
of World Economy and Diplomacy

CROSS-BORDER FLOW OF PERSONAL INFORMATION: INTERNATIONAL PRACTICES

Abstract. The cross-border flow of personal information has become a critical issue in the digital age, shaped by varying legal frameworks and priorities across jurisdictions. This paper examines the regulatory approaches of four major players—the United States, the European Union (EU), Russia, and China—highlighting their distinct strategies, strengths, and challenges. The U.S. adopts a market-oriented, fragmented model that prioritizes innovation but faces criticism for weak privacy protections and extraterritorial surveillance. The EU, through its General Data Protection Regulation (GDPR), establishes a rights-based, unified framework that sets global privacy standards but struggles with high compliance costs and enforcement inconsistencies. Russia enforces a defensive, sovereignty-driven model with strict data localization and geopolitical controls, which enhances national security but leads to technological isolation. China balances security and development through its "three-pillar" framework (Cybersecurity Law, Data Security Law, and Personal Information Protection Law), promoting regulated data flows while advancing its global influence via initiatives like the "Digital Silk Road." Despite their differences, all four jurisdictions face challenges in balancing privacy, security, and economic interests. The paper concludes with recommendations for fostering international cooperation, enhancing transparency, and leveraging technology to build a more interoperable and equitable global data governance framework.

Keywords: Cross-Border Data Flows; Personal Information Protection; GDPR; Data Sovereignty.

Annotatsiya. Shaxsiy ma’lumotlarning chegaralararo oqimi raqamli davrda muhim masalaga aylandi, bu esa turli yurisdiktsiyalar o‘rtasida farqlanuvchi huquqiy ramkalar va ustuvorliklar bilan shakllangan. Ushbu maqola AQSh, Yevropa Ittifoqi (YI), Rossiya va Xitoy kabi to‘rt asosiy o‘yinchining tartibga solish yondashuvlarini o‘rganadi va ularning o‘ziga xos strategiyalari, kuchli va zaif tomonlarini ko‘rsatadi. AQSh innovatsiyani ustun qo‘yadigan bozor yo‘nalishidagi parchalanadigan modelni qabul qiladi, ammo zaif maxfiylik himoyasi va ekstraterritorial kuzatuvlar uchun tanqidga uchraydi. Yevropa Ittifoqi, Umumiy Ma’lumotlarni Himoya Qilish Qoidasi (GDPR) orqali, global maxfiylik standartlarini belgilovchi huquqiy asosga ega, birlashtirilgan ramka yaratadi, lekin yuqori muvofiqlik xarajatlari va ijro etishdagi nomuvofiqliklar bilan kurashmoqda. Rossiya qat'iy ma’lumotlarni joylashtirish va geosiyosiy nazorat bilan bog‘liq mudofaa va suverenitetga asoslangan modelni amalga oshiradi, bu esa milliy xavfsizlikni oshiradi, lekin texnologik izolyatsiyaga olib keladi. Xitoy esa "uch ustunli" ramkasi (Kiberxavfsizlik Qonuni, Ma’lumotlarni Xavfsizligi Qonuni va Shaxsiy Ma’lumotlarni Himoya Qilish Qonuni) orqali xavfsizlik va rivojlanishni muvozanatlaydi, tartibga solingan ma’lumot oqimlarini rivojlantiradi va "Raqamli Ipak Yo‘li" kabi tashabbuslar orqali global ta’sirini oshiradi. Ularning farqlanishlariga qaramay, to‘rt yurisdiktsiya ham maxfiylik, xavfsizlik va iqtisodiy manfaatlarni muvozanatlashda qiyinchiliklarga duch kelmoqda. Maqola xalqaro hamkorlikni rivojlantirish, shaffoflikni oshirish va texnologiyalardan foydalangan holda global ma’lumotlarni boshqarish tizimini yanada o‘zaro bog‘liq va adolatli qilish bo‘yicha tavsiyalar bilan yakunlanadi.

Kalit so‘zlar: Chegaralararo ma’lumot oqimlari; shaxsiy ma’lumotlarni himoya qilish; GDPR; ma’lumot suvereniteti.

Аннотация. Трансграничный поток персональной информации стал критически важной проблемой в цифровую эпоху, формируемой различными правовыми рамками и приоритетами в разных юрисдикциях. В данной статье рассматриваются регуляторные подходы четырех основных игроков — Соединенных Штатов, Европейского Союза (ЕС), России и Китая — подчеркиваются их отличительные стратегии, сильные и слабые стороны, а также вызовы. США используют ориентированную на рынок фрагментированную модель, которая придает приоритет инновациям, но сталкивается с критикой за слабую защиту конфиденциальности и экстерриториальный надзор. ЕС, с помощью Общего регламента по защите данных (GDPR), устанавливает основанную на правах единую структуру, которая задает глобальные стандарты конфиденциальности, но сталкивается с высокими затратами на соблюдение и несоответствиями в правоприменении. Россия применяет защитную модель, ориентированную на суверенитет, с жесткими требованиями к локализации данных и геополитическими контролями, что усиливает национальную безопасность, но ведет к технологической изоляции. Китай балансирует безопасность и развитие через свою "трехстороннюю" структуру (Закон о кибербезопасности, Закон о безопасности данных и Закон о защите персональной информации), способствуя регулируемым потокам данных, одновременно продвигая свое глобальное влияние через такие инициативы, как "Цифровой Шелковый путь". Несмотря на различия, все четыре юрисдикции сталкиваются с проблемами в балансировке конфиденциальности, безопасности и экономических интересов. В статье представлены рекомендации по содействию международному сотрудничеству, повышению прозрачности и использованию технологий для создания более совместимой и справедливой глобальной структуры управления данными..

Ключевые слова: трансграничные потоки данных; защита персональной информации; GDPR; суверенитет данных.

Introduction

The development of internet technology has made the collection, use, and disclosure of personal information increasingly accessible, leading to a continuous cross-

border flow of personal data. Due to differences in the level of development of network services and data technologies among countries, cross-border data flows involve multiple issues in the fields of law, economy, security, and culture. Different legal systems prioritize different values: some focus on the protection of individual rights, while others emphasize the economic value of information circulation. Currently, cross-border data flows are closely tied to commercial practices such as e-commerce and digital trade [1]. However, the extent to which cross-border data flows comply with the World Trade Organization (WTO) principles of national treatment and most-favored-nation treatment remains unclear, and the validity of "cultural exceptions" to restrict data flows is questionable [2].

The attitudes of countries toward cross-border data flows are influenced by the domestic legal definitions of personal information and the current international consensus. This paper will review the regulatory approaches of major countries and regions, including the United States, the European Union, Russia, and China, and propose a more suitable operational model.

Analysis and results

1. Definition of Key Terms

Personal Information

Personal information refers to any data that can identify a specific individual, either alone or in combination with other information. It includes but is not limited to names, identification numbers, contact information, and biometric data. The core characteristic of personal information is identifiability, meaning it can directly or indirectly identify a specific individual [3].

Cross-Border Flow of Personal Information

In international documents, the term "cross-border flow" is often used, corresponding to "cross-border transfer" in APEC and OECD documents. China's Personal Information Protection Law uses the term "cross-border provision," which is scientifically justified for two reasons: first, it reflects the active provision of data by domestic data controllers to foreign entities; second, it encompasses not only the physical transfer of data but also the provision of access to data stored domestically to foreign entities or individuals.

Historically, the international community has placed great emphasis on the cross-border movement of goods, services, intellectual property, capital, and people, while largely neglecting the cross-border flow of data. This is closely related to the limited technological development and the lack of large-scale, commercial applications of data at the time. Specifically, many important agreements under the WTO address the cross-border movement of goods and services; the World Intellectual Property Organization (WIPO) seeks to establish minimum protection standards for intellectual property to facilitate its global flow; the movement of people involves immigration and visa policies, while the flow of capital is often strictly controlled by national foreign exchange systems. In contrast, cross-border data flows have not received sufficient attention, and there are limited international coordination efforts in this area, with only a few free trade agreements including rules on personal information protection and cross-border data flows. Below, the author will compare the legislative, enforcement, and judicial practices of the United States, the European Union, Russia, and China.

2. The U.S. Practice: Market-Oriented Governance with Fragmented Regulation

The regulation of cross-border data flows in the United States is not based on a single law but is achieved through a three-dimensional model of "regulatory agency coordination + judicial case law supplementation + industry standard guidance," characterized by a "fragmented" approach. The U.S. lacks a unified federal data protection law but has built a unique governance system through industry self-regulation, a combination of federal and state laws, and international agreements [4]. Its legal practices are market-oriented, focusing on balancing data flows with national security and privacy protection.

At the federal level, the Privacy Act of 1974 regulates the collection and use of personal information by federal agencies but does not explicitly address cross-border data transfers [5]. Its core principles, such as data minimization, provide a foundation for subsequent legislation. Sector-specific laws include the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to protect customer information and allows cross-border transfers with user notification; the Health Insurance Portability and Accountability Act (HIPAA), which restricts the cross-border transfer of medical information and requires the signing of business associate agreements; and the Children's Online Privacy Protection Act (COPPA), which prohibits the cross-border transfer of children's data without parental consent. In terms of national security legislation, the Foreign Intelligence Surveillance Act (FISA) authorizes the government to access foreign data for national security purposes, leading to conflicts with EU laws. The Federal Trade Commission Act (FTC Act) empowers the Federal Trade Commission (FTC) to prohibit "unfair or deceptive practices" and conduct ex-post oversight of corporate misconduct in cross-border data flows.

At the state level, legislative breakthroughs include California's Consumer Privacy Act (CCPA/CPRA), which grants consumers rights such as the right to know and the right to delete, requiring businesses to disclose cross-border data transfer practices. The CPRA, which took effect in 2023, further establishes a privacy protection agency to strengthen cross-border data regulation. Virginia's Consumer Data Protection Act (VCDPA) requires businesses to conduct data protection assessments, including assessments of cross-border transfer risks [6].

In terms of international data transfer mechanisms, the EU-U.S. data transfer framework has evolved from the Safe Harbor Agreement (2000-2015) to the Privacy Shield Agreement (2016-2020) and, most recently, the EU-U.S. Data Privacy Framework in 2023, which introduces new safeguards such as restrictions on intelligence access and the establishment of a Data Protection Review Court (European Commission, 2023). The APEC Cross-Border Privacy Rules (CBPR) system, promoted by the United States, facilitates regional data flows through certification mechanisms but is less stringent than the EU's adequacy decisions (APEC, 2021). Bilateral judicial assistance agreements under the CLOUD Act framework allow for cross-border access to law enforcement data with coun-

tries such as the United Kingdom and Australia (DOJ, 2019) [7].

The U.S. model is characterized by flexibility and industry self-regulation but faces three major challenges: conflicts between federal and state laws, which increase corporate compliance costs due to varying privacy standards across states; insufficient international interoperability, as the EU Court of Justice has repeatedly rejected the adequacy of U.S. data protection, affecting transatlantic data flows; and the tension between surveillance laws and privacy rights, as the mass surveillance authorized under Section 702 of FISA continues to erode international trust (Privacy & Civil Liberties Boa.

3. The EU Practice: Rights-Based Unified Regulation

The European Union has established the world's strictest regulatory framework for cross-border data flows through the General Data Protection Regulation (GDPR). Its core feature is the recognition of data privacy as a fundamental right (Article 8 of the EU Charter of Fundamental Rights) and the establishment of a "prohibition in principle—exceptions permitted" mechanism for cross-border data transfers (GDPR Article 44). Compared to the market-oriented approach of the United States, the EU uses "adequate protection levels" as a benchmark and achieves extraterritorial legal effects through legislative, judicial, and administrative coordination, profoundly influencing global data governance rules [12].

From a legislative perspective, the most notable is the General Data Protection Regulation (GDPR). Chapter V of the GDPR (Articles 44-50) specifically addresses cross-border data transfer rules, stipulating that the legality of transfers depends on three conditions: adequacy decisions, where the European Commission determines that a third country provides an "adequate" level of data protection (e.g., Japan, South Korea) (GDPR Article 45); appropriate safeguards, including Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and certification mechanisms (GDPR Article 46); and specific exceptions, such as explicit consent from the data subject or the necessity of fulfilling a contract (GDPR Article 49). Complementing the GDPR, the Law Enforcement Directive (LED) and the ePrivacy Directive impose additional restrictions on cross-border access to communication data by law enforcement agencies, requiring "purpose limitation" and "necessity testing" (Directive 2016/680 Article 35; Directive 2002/58/EC Article 4). Supplementary mechanisms include guidelines from the European Data Protection Board (EDPB), which publishes technical documents such as the Recommendations on Supplementary Measures for Cross-Border Data Transfers (2021), requiring companies to assess the impact of third-country laws on data transfers. The Data Governance Act (DGA) and the Data Act introduce new rules for cross-border sharing of public sector data and restrict access to EU data by non-EU governments (DGA Article 5).

The main characteristics of the EU's approach to cross-border data transfers are as follows:

Judicial activism drives the evolution of rules. The Schrems I and II cases saw the Court of Justice of the European Union (CJEU) overturn the EU-U.S. Safe Harbor and Privacy Shield agreements, establishing the "essential equivalence" standard for review (C-362/14; C-311/18). In the Meta Ireland case (2023), the CJEU ruled that relying solely on SCCs is insufficient for compliance and that additional technical measures, such as encryption and data anonymization, must be implemented (Case C-252/21).

The "Brussels Effect" and rule exportation. The EU's adequacy decisions have influenced data protection laws in other jurisdictions, such as Brazil's General Data Protection Law (LGPD) and South Africa's Protection of Personal Information Act (POPIA), both of which draw on the GDPR's cross-border transfer framework. The extraterritorial reach of the GDPR under Article 3, which applies to foreign companies offering goods or services to EU residents, has significantly increased compliance costs for Chinese and U.S. tech companies (e.g., the ban on Google Analytics in Austria, DSB 2022) [14].

Innovation in regulatory tools. The EU requires companies to conduct Transfer Impact Assessments (TIAs) to systematically evaluate the risks of third-country government access to data (EDPB 2021/09). The modular SCCs introduced in 2021 differentiate between four scenarios—controller-to-processor, processor-to-subprocessor, etc.—enhancing flexibility (Commission Implementing Decision 2021/914).

Overall, the EU's approach has both strengths and challenges.

Strengths:Raising global privacy standards: Companies like Microsoft and Amazon have been forced to redesign their global product architectures (e.g., Azure EU Data Boundary).

Strengthening personal data sovereignty: Article 48 of the GDPR restricts foreign courts from directly accessing EU data, countering the jurisdictional conflicts posed by the U.S. CLOUD Act [15].

Challenges:High compliance costs: Small and medium-sized enterprises (SMEs) struggle to bear the costs of SCCs and supplementary measures, leading to reduced efficiency in data flows (Bertuzzi, 2023).

Fragmented enforcement across member states: The Irish Data Protection Commission's (DPC) slow penalties for Meta contrast sharply with the Hamburg Data Protection Authority's (DPA) strict enforcement against Google (Cellan-Jones, 2023).

Geopolitical instrumentalization: The EU has used data flow restrictions as leverage in the U.S.-China tech competition (e.g., excluding Huawei from the 5G cybersecurity toolbox) [16].

Future directions:Promoting the development of "trusted data spaces": The EU is building a data infrastructure alliance led by the GAIA-X project.

Dynamic adjustment of adequacy lists: Human rights protection levels are being incorporated into assessments (e.g., the 2024 adequacy review of Israel includes considerations of the Gaza conflict) [17].

4. Russia's Practice: Sovereignty-Oriented Strict Control

Russia has established a highly restrictive framework for cross-border data flows through the Federal Law on Personal Data (No. 152-FZ). Its core logic is to treat personal information as a national sovereignty resource, em-

phasizing data localization requirements and government review of cross-border transfers. This model reflects Russia's strategic goal of countering Western sanctions and strengthening domestic internet governance (the "sovereign internet" policy), contrasting sharply with the EU's rights-based approach and the U.S.'s market-oriented model.

Russia's legal framework consists of foundational legislation and supplementary rules and regulatory bodies.

Foundational legislation:The Federal Law on Personal Data (No. 152-FZ), amended in 2015 (Article 18(5)), establishes key rules:Mandatory data localization: Operators collecting personal data of Russian citizens must store it in databases located within Russia.Conditional cross-border transfers: Transfers are only permitted to countries on the "adequacy whitelist" or based on exceptions such as the data subject's written consent or the fulfillment of international treaties.

The Sovereign Internet Law (No. 90-FZ) authorizes the creation of national internet infrastructure (e.g., RuNet), restricting cross-border data routing autonomy and ensuring the government can disconnect from the global internet if necessary (Klimenko, 2020) [19].

Supplementary rules and regulatory bodies:

Adequacy whitelist system: The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) evaluates the data protection levels of other countries. Currently, only members of the Eurasian Economic Union (EAEU), such as Belarus and Kazakhstan, are included (Roskomnadzor Order No. 274, 2021).

Cross-border transfer approval process: Companies must submit the purpose of the transfer, the type of data, and the legal environment of the recipient country to Roskomnadzor for approval before transferring data (No. 152-FZ Article 12).

Special restrictions:State secrets and sensitive data: The State Secrets Law (No. 5485-1) prohibits the cross-border transfer of any personal information containing state secrets.

Financial data: The Central Bank of Russia requires payment system data to be processed entirely within Russia (Bank of Russia Regulation No. 382-P, 2017).

In practice, Russia's approach is characterized by thefollowing: Extraterritorial jurisdiction and enforcement deterrence.LinkedIn blocking case (2016): Roskomnadzor blacklisted LinkedIn for refusing to localize Russian user data, making it the first international social platform to be banned in Russia (Roskomsvoboda, 2016).

Google and Meta fines (2022): Both companies were fined over 70 billion rubles for failing to remove "illegal content" and violating data localization requirements (Roskomnadzor, 2022) [20].

Deep integration with geopolitics:Building a "data sovereignty alliance": Russia signed a Cross-Border Data Flow Cooperation Agreement with Iran in 2023, allowing direct transfers of financial and energy data between the two countries, bypassing the SWIFT system (MID, 2023).

Sanctions countermeasures: Russia restricts Western companies from transferring Russian citizens' data to their home countries, forcing companies like Microsoft and SAP to establish local data centers (Vedomosti, 2022) [21].

Strengthening technical compliance measures:

Mirror server requirements: Foreign platforms must set up physical servers in Russia and synchronize all user data (e.g., Telegram was unblocked after partial compliance).

Encrypted transfer permits: If data is encrypted using Russian-certified algorithms (e.g., GOST 34.12-2015), companies can apply for simplified approval processes (FSTEC Order No. 239, 2020) [22].

In summary, Russia's approach to cross-border data transfers faces contradictions and challenges under its defensive system.

Advantages:Strengthening digital sovereignty: Reducing reliance on Western internet services has significantly increased the market share of domestic platforms like Yandex and VK (Statista, 2023).

Ensuring national security: Data localization blocks foreign intelligence agencies from direct access (e.g., strict scrutiny of cloud service providers after the Snowden incident).

Challenges:Exodus of international companies: Companies like Apple and Amazon have closed cloud services in Russia due to high compliance costs, hindering the digital transformation of SMEs (Forbes Russia, 2023).

Selective enforcement: Lenient scrutiny of companies from "friendly countries" undermines the credibility of the rules (Carnegie, 2022).

Russia's defensive cross-border data flow regulatory system, built on mandatory localization, government review, and geopolitical instrumentalization, strengthens state control over data but leads to technological isolation, corporate outflows, and regulatory fragmentation. In the future, Russia may alleviate pressure through regional alliances and "data diplomacy," but the sustainability of its system depends on the evolution of the international political and economic landscape.

5. China's Practice: Balancing Security and Development

China has gradually established a regulatory framework for cross-border data flows centered on the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law (PIPL). This framework emphasizes the balance between data sovereignty, national security, and the protection of personal information rights. Drawing on the EU's concept of "adequate protection" while adapting it to China's national conditions, the framework reflects the principles of "classified and hierarchical management" and "risk control." China's legal practices not only serve the needs of domestic digital economic development but also promote international rule-making through initiatives such as the "Digital Silk Road."

China's Legal Framework

China's legal system for cross-border data flows is based on the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law (PIPL), supplemented by a series of supporting rules and industry guidelines, forming a multi-level and multi-dimensional regulatory framework.

The Cybersecurity Law, enacted in 2017, introduced

the requirement for critical information infrastructure (CII) operators to localize data storage, explicitly prohibiting the illegal transfer of personal information and important data overseas. This provision laid the foundation for subsequent legislation.

The Data Security Law, enacted in 2021, established a data classification and hierarchical protection system, requiring security assessments for cross-border data transfers to ensure risk control.

The Personal Information Protection Law (PIPL), effective in 2021, is the cornerstone of this framework. It includes a dedicated chapter on cross-border data transfers, stipulating that such transfers must meet one of the following conditions: passing a security assessment organized by the Cyberspace Administration of China (CAC), obtaining personal information protection certification, or signing a standard contract. These provisions provide diverse compliance pathways for businesses while strengthening the government's regulatory capabilities over data flows.

Supporting Rules and Regulatory Bodies

The Measures for Security Assessment of Cross-Border Data Transfers, issued in 2022, clarify the scope, procedures, and standards for security assessments. Companies processing personal information of more than 1 million individuals or transferring more than 1TB of data must undergo such assessments.

The Measures for Standard Contracts for Cross-Border Data Transfers, effective in 2023, provide a simplified compliance pathway for small and medium-sized enterprises (SMEs), requiring companies to file contracts with regulators.

The Personal Information Protection Certification Rules, issued in 2022, are implemented by the China Cybersecurity Review Technology and Certification Center (CCRC) and cover cross-border data transfer scenarios.

Sector-Specific Restrictions

China has also introduced specialized regulations for sensitive data in specific sectors. For example, the People's Bank of China requires payment institutions to store domestic transaction data within China, while the Ministry of Natural Resources prohibits the cross-border transfer of high-precision map data. These industry-specific rules further refine the management of cross-border data flows.

Characteristics of China's Legal Practices

China's approach to cross-border data flows is characterized by three main features: classified and hierarchical management, extraterritorial jurisdiction, and international cooperation.

Classified and Hierarchical Management: China differentiates between "important data" and general personal information, imposing strict localization requirements on the former while providing multiple compliance pathways for the latter. Industry-specific guidelines, such as the Regulations on the Management of Automotive Data Security, further clarify data types and risk assessment standards.

Extraterritorial Jurisdiction: China has strengthened enforcement deterrence through high-profile cases. For example, Didi Global was fined 8.026 billion yuan for illegally transferring user data overseas, the largest penalty under PIPL. ByteDance was also required to migrate U.S. user data of TikTok to Oracle servers and undergo security reviews by Chinese authorities.

International Cooperation: China promotes the "Digital Silk Road" initiative, signing cross-border data flow cooperation agreements with ASEAN and Central and Eastern European countries to advance the concept of "data sovereignty." Additionally, China's accession to the Digital Economy Partnership Agreement (DEPA) facilitates the mutual recognition of cross-border data flow rules, enhancing its influence in international rule-making.

Evaluation: Strengths and Challenges

China's legal framework for cross-border data flows has achieved significant results in safeguarding national security and promoting digital economic development, but it also faces challenges.

Strengths:Balancing Security and Development: .The strict localization requirements for important data effectively protect national security, while the diverse compliance pathways provide flexibility for businesses engaged in cross-border activities.

Rule Exportation: Through initiatives like the "Digital Silk Road" and DEPA, China is gradually exporting its domestic rules to the international stage, enhancing its influence in global data governance.

Challenges:High Compliance Costs: The complex and lengthy security assessment process imposes significant compliance burdens, particularly on SMEs.Lack of Transparency in Enforcement: Some enforcement cases, such as the Didi penalty, lack detailed legal justifications, which may undermine foreign companies' confidence in the Chinese market.Insufficient International Interoperability: Conflicts between China's rules and those of the EU (e.g., GDPR) and the U.S. (e.g., CLOUD Act) hinder smooth cross-border business cooperation.

Future Directions:Optimizing Security Assessment Processes: Pilot programs for a "whitelist" system are being introduced to simplify approval processes for low-risk data transfers.

Strengthening International Cooperation: China is leveraging multilateral mechanisms such as RCEP and CPTPP to promote mutual recognition of rules and reduce trade barriers.

In summary, China has established a regulatory system for cross-border data flows that balances security and flexibility through its "three-pillar" legislative framework. While it meets the needs of domestic digital economic development and promotes international rule-making, challenges such as high compliance costs, lack of transparency in enforcement, and insufficient international interoperability remain. In the future, China needs to further optimize assessment processes and strengthen international cooperation to achieve a dynamic balance between security and development.

Conclusion

By comparing the legal practices of major countries such as the United States, the European Union, Russia, and China regarding the cross-border flow of personal information protection, the following observations can be made:

The United States adopts a market-oriented approach, relying on industry self-regulation and fragmented legisla-

tion. Through the CLOUD Act and bilateral agreements, it extends data jurisdiction. Its strengths lie in high flexibility and adaptability to the innovation needs of the digital economy. However, the fragmented federal and state laws increase compliance costs, and large-scale surveillance has triggered an international trust crisis.

The European Union, with the General Data Protection Regulation (GDPR) as its cornerstone, has established a rights-based, strict regulatory system. Through adequacy decisions and judicial activism (e.g., the Schrems case), it strengthens the extraterritorial influence of its rules. The system's advantage lies in elevating global privacy standards, but high compliance costs and enforcement inconsistencies among member states weaken internal unity.

Russia employs a "defensive governance" model, mandating data localization through the Federal Law on Personal Data and using geopolitical tools to restrict data flows from Western companies. While this model strengthens digital sovereignty, technological isolation and the exodus of enterprises have diminished the vitality of its digital economy.

China, guided by the principle of "balancing security and development," has built a classified and hierarchical management system through the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law (PIPL), balancing national security and commercial needs. Its strengths include rule-exporting capabilities (e.g., the "Digital Silk Road"), but insufficient international interoperability and transparency in enforcement hinder cross-border cooperation. [28]

At the legislative level, it is essential to build a compatible framework and promote the mutual recognition of multi-level rules. Data flow provisions should be incorporated into regional agreements (e.g., CPTPP, RCEP), and a hybrid model of "equivalence certification + risk assessment" should be explored to reduce regulatory conflicts. Classification and grading standards should be refined, drawing on China's mechanism of distinguishing between "important data" and "general data," to clarify transmission conditions for data of different risk levels and reduce corporate compliance burdens.

At the enforcement level, collaboration and transparency should be enhanced. A cross-border law enforcement cooperation mechanism should be established, modeled after the dispute resolution body under the EU-U.S. Data Privacy Framework, to coordinate cross-border investigations and resolve enforcement conflicts. Transparency in enforcement should be improved by requiring regulatory agencies to disclose the legal basis and procedures for penalties in typical cases (e.g., the Cyberspace Administration of China's release of security assessment guidelines), thereby enhancing predictability for businesses.

At the technical level, privacy-enhancing technologies (PETs) should be supported, and encryption and anonymization technologies should be promoted. Technical compliance should be integrated into legal standards; for example, the "pseudonymization" recognized by the EU GDPR can serve as a supplementary measure for cross-border data transfers. Cross-border data flow monitoring tools should be developed, leveraging blockchain technology to enable data tracking and ensure the auditability of transmission processes (e.g., the cross-border payment pilot by the Digital Currency Research Institute of the People's Bank of China).

At the international governance level, the weaponization of rules should be avoided, and the geopolitical use of data flows should be restricted. Platforms such as the WTO should regulate the abuse of "national security exceptions" to prevent data localization requirements from becoming trade barriers. Developing countries should be supported in participating in rule-making, and a universal data governance fund should be established under the United Nations framework to help technologically disadvantaged countries enhance their regulatory capabilities.

Current Trends and Future Directions. Currently, global rules on cross-border personal data transfers exhibit a trend of "value divergence": the U.S.-EU rivalry reflects the tension between market freedom and rights protection, while the China-Russia model highlights the prioritization of digital sovereignty and national security. Future regulations must seek a dynamic balance between security and efficiency, sovereignty and cooperation. Legislators should abandon the "zero-sum game" mindset and, through technological empowerment, rule mutual recognition, and multilateral collaboration, promote the establishment of a "controlled globalization" order for data flows, ultimately achieving a win-win outcome for individual rights, corporate interests, and public security.

References

1. Shi, Y. W. (2020). International trade rules in cross-border data flows: Regulation, compatibility, and development. Comparative Law Review, 4, 173–184.

2. Tan, G. F. (2021). Exceptions in digital trade regulation. Hebei Law Science, 6, 102–120.

3. Personal Information Protection Law of the People's Republic of China, Article 4 (2021).

4. Wu, X. (2022). Cross-border data law enforcement in the cloud era: U.S. CLOUD Act and China's approach. Local Legislation Research, 5, 116.

5. CLOUD Act, Pub. L. No. 115-141, 132 Stat. 1213 (2018).

6. California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (2018).

7. European Commission. (2023). Commission Implementing Decision on the EU-U.S. Data Privacy Framework. Brussels: EU Publications Office.

8. Wang, H., & Zhou, B. W. (2023). The extraterritorial expansion of U.S. long-arm jurisdiction and its mitigation. Journal of North China University of Science and Technology (Social Science Edition), 23(2), 13–19.

9. Liu, S. X. (2019). Cross-border personal data flows in the context of globalization. China Finance, 23, 68–70.

10. Li, Y. H. (2021). Cross-border data flow regulation between the EU and the U.S. after the Privacy Shield case: The future of soft data localization mechanisms and the innovation of standard contractual clauses. European Studies, 39(6), 25–49.

11. Jin, J. (2018). The EU General Data Protection Regulation: Evolution, key points, and ambiguities. Proceedings of the 12th Annual Conference of the

European Law Research Association of China, 181–189.

12. Wang, A. L., & Da, N. S. (2020). China’s voice on "cyber sovereignty" and its international recognition. Journal of Dalian University of Technology (Social Sciences), 6, 1–8.

13. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer International Publishing AG.

14. Kuner, C. (2020). The international dimension of the GDPR. Oxford University Press.

15. Schwartz, P. M. (2019). Global data privacy: The EU way. NYU Law Review, 94(3), 771–818.

16. Federal Law No. 152-FZ "On Personal Data" (2006, amended 2015).

17. Roskomnadzor. (2021). Order No. 274 on Approval of Cross-Border Data Transfer Procedures. Moscow: Official Gazette.

18. Klimenko, E. (2020). Russia’s sovereign internet law: Origins and implications. Chatham House Report.

19. Soldatov, A. (2022). Digital iron curtain: Russia’s data localization regime. Journal of Cyber Policy.

20. Belfer Center. (2021). Encryption standards and geopolitics: The case of GOST. Harvard Kennedy School.

21. Carnegie Endowment. (2022). Selective enforcement in Russia’s digital economy. Moscow: Carnegie.ru.

22. Zhang, J. P. (2016). Cross-border data transfer rules under China’s Cybersecurity Law. Politics and Law,12, 137–148.

23. Zhang, X. B. (2018). Major contradictions in the legislation of China’s Personal Information Protection Law. Journal of Jilin University (Social Sciences Edition), 5, 45–55.

24. Zhao, H. L. (2022). Conflicts and strategies in international governance of personal information protection from a data sovereignty perspective. Contemporary Law Review, 4, 82–91.