ISSN 2616-7433 Vol. 4, Issue 7: 53-58, DOI: 10.25236/FSST.2022.040710

Challenges faced by Russian companies involved in cross-border data flows

Wang Anna

Institute of Foreign Language, Nanchang University, Nanchang, China
anna18070595967@163.com

Abstract: *Against the backdrop of the liberalisation of international data flows, Russia has been strengthening its data localisation policies for the purposes of safeguarding its national security and protecting the rights of its citizens to personal data, and the corresponding costs of non-compliance are rising. In recent years, cases such as Google being fined heavily by the Russian authorities have raised awareness of the need for companies involved in Russia to comply with cross-border data regulations in Russia. The differences in data legislation between Russia and other countries have created new challenges in terms of legal risks and costs for companies involved in Russia, and companies should face up to the challenges of data compliance and be prepared to avoid data compliance risks.*

Keywords: *Russia; Cross-border Flows; Data Localisation; Compliance; Information Security*

1. Introduction

The Russian digital economy is growing rapidly thanks to domestic policies and market foundations, and at the same time, the Russian digital economy market is less competitive than the European and American markets, making Russia an increasingly popular investment market for multinational companies. As new communication technologies such as the Internet of Things, cloud computing and big data make the development of the data economy increasingly dependent on the flow of data, it is inevitable that when entering the Russian market, companies need to fully understand the relevant provisions of the Russian data legislation and take into account the corresponding legal risks.

At present, research on the cross-border data sector is mainly focused on the two major economic entities, namely the US and the EU, and there is not much literature that comprehensively reviews and analyses measures in the field of data flow in Russia. In view of this, this article attempts to summarise the characteristics of Russian data legislation, summarise the legislative trends and outline the challenges faced by Russian companies in the area of two-way data compliance, taking into account several case studies, with a view to providing reference for Russian companies to understand the relevant Russian laws and promote the stable development of Russian companies.

2. The Russian paradigm of cross-border data flows

2.1 Basic strategies for cross-border data flows in Russia

2.1.1 Taking the maintenance of national security as the starting point

In 1995, President Yeltsin signed the Concept for the Construction and Development of a Unified Information Space and National Information Resources in Russia, putting forward for the first time the idea of building a unified information space for the whole of Russia. Since then, Russia has been gradually building a national information society through documents such as the Outline of State Information Policy and the Concept of Russian Information Policy, and has initially incorporated information security into the scope of national security management. Looking at Russia's early national information security legal system, Russia attached great importance to the long-term guiding role of programmatic documents in the field of information legislation, which provided direction for the subsequent refinement of information security legislation. The Law on Information, Informatization and Information Protection (hereinafter referred to as the "Information Protection Law"), enacted in the same period, was guided by such programmatic documents. The Law regulates the legal relations arising from the process of information processing and for the first time specifies that information

ISSN 2616-7433 Vol. 4, Issue 7: 53-58, DOI: 10.25236/FSST.2022.040710

resources are part of property and the object of ownership, thus establishing the importance of information resources in law.

Since entering the 21st century, information resources and their foundations have become an important weapon for the development of all countries, and the effective functioning of national information systems is a necessary condition for the maintenance of national security. Based on this, in 2006 the Security Council of the Russian Federation adopted the first edition of the Doctrine of State Information Security (hereinafter referred to as the Doctrine), which explicitly developed cyber information resources and formally included information security in the scope of national security. the second edition of the Doctrine, promulgated in 2016, further clearly stated the national interests of the Russian Federation in the field of information security, namely: safeguarding the rights and freedoms of citizens The Russian Federation's national security interests in the field of information security are: safeguarding the rights and freedoms of citizens, safeguarding the security of the information infrastructure, safeguarding the development of the domestic information technology and electronics industry, safeguarding security in the cultural sphere through the use of information technology, and safeguarding sovereignty in the information sphere. Comparing the two editions of the Doctrine, it can be seen that, with regard to information security, Russia's strategy has shifted from proposing development to protecting the national interests it involves. This shows, on the one hand, the increasing importance that Russia attaches to national information security and, on the other hand, reflects the direction of development in which Russia is constantly strengthening its data sovereignty.

In May 2014, the Russian Information Act was amended to include requirements for data storage in the country under the heading "Obligations of Internet information dissemination organisations". In May 2014, the Russian Information Law was amended to include requirements for storage in the country under the heading "Obligations of Internet Information Dissemination Organisations", thus formally bringing data security into the national information security sphere.

It would appear that Russian data legislation has been shaped by the basic framework for building national information security, and that its basic strategy for maintaining national information security has determined the direction of its legislation to prioritise the maintenance of data security in its data legislation.

2.1.2 Emphasis on the protection of personal data security

The right to freedom of information is enshrined in a number of Russian legal instruments. Article 29 of the Constitution states that "everyone has the right to collect, acquire, transmit, produce and disseminate information by any lawful means". The Law on the Protection of Information, adopted in 1995, stipulates that "personal information is confidential and the collection, keeping, use and dissemination of information concerning private life, as well as information concerning private secrets of natural persons, family secrets, letters, telephone calls, mail, telegrams and other secrets are prohibited without the permission of the person concerned". In addition, the 1997 Russian National Security Concept includes "the right and freedom of citizens to access and use information" as part of the State's interest in information security. One of the most influential laws in the field of personal information is the 2006 Law of the Russian Federation on Personal Data (hereinafter referred to as the "Personal Data Law"), which recognises the legitimate rights and interests of personal information and privacy at the legal level, and provides guidelines for information processors throughout society, with regard to the processing of personal information. Personal data is the basis for generating information exchange between countries and an important tool for multinational companies to open up new markets, and establishing citizens' right to information is an important prerequisite for the protection of their personal data security. Russia has established legal protection of citizens' right to information through its policies, constitution, laws and regulations, and at the same time has taken legal measures to ensure the security of its information as it continues to open its markets to the outside world. The Personal Data Act is important for the exchange of information, the security of national information and the economic development of the country.

The Personal Data Act, introduced in 2006, stipulates that before personal data can be transferred across borders, the data holder or processor must confirm that the recipient's country is able to ensure the security of the data. 2015 saw amendments to the Personal Data Act which clearly state that Personal data of Russian citizens can only be stored on servers in Russia and copies of personal data can only be stored on servers abroad during the time of use, to further strengthen data localisation[1] . As a result of the Act, Ebay has moved its servers from Switzerland to a US Internet company in Russia[2] . Apple, for its part, has partnered with Moscow-based internet company IXcellerate to store data on Russian Apple users' cloud services on each other's servers, providing a new model for

ISSN 2616-7433 Vol. 4, Issue 7: 53-58, DOI: 10.25236/FSST.2022.040710

Russian-related companies to work with the Russian government to localise their data. In contrast, Linkedln has been blacklisted by Russian internet regulators and blocked by Russian internet operators for refusing to transfer Russian user data to servers in Russia, and internet companies, including Facebook and Twitter, are in danger of being completely banned for breaking the same rules.

2.2 Analysis of the characteristics and trends of cross-border data flows in Russia

2.2.1 Firmly implement a strict data localisation policy

"Data localisation" refers to a country's requirement that data generated or collected in its territory be stored in its territory and that cross-border flows be restricted or prohibited in order to safeguard its national security and trade in the digital economy.

In 2014, the basic framework for data localisation in Russia was established by Federal Decrees Nos. 97 and 242. Under Federal Decree No. 97, internet service providers are required to store all types of electronic information received in the Russian Federation for a period of six months, and internet information dissemination services are required to store such information in the Russian Federation.[3] . In the same year, Federal Decree No. 242 "On Amendments to the Series of Laws of the Russian Federation "On Further Clarification of the Regulation of the Processing of Personal Data on the Internet", once again emphasised that information processors should store databases on the territory of the Russian Federation[4] . In 2015, the Personal Data Act required data processors to inform the Russian Federation before processing data of Information on the location of databases containing the personal data of Russian citizens. Since then, Russia has continued to strengthen its data localisation policy through successive acts that have weakened the degree of freedom of movement of its data across borders. For Russia, where national cyber security is under constant attack, data localisation policies are more conducive to safeguarding national security and citizens' data rights.

In the context of globalisation, data has great economic value and there is a contradiction between restricting the flow of data and developing economic trade. For companies involved in Russia, especially those with a high dependence on internet data transmission, Russia's data localisation policy can hinder their development to some extent.

2.2.2 High priority given to the protection of data rights of Russian citizens

Since the enactment of the Information Act in 1995, the Russian Federation has legally established the right of Russian citizens to information and privacy in the online sphere. In order to comprehensively protect the data rights of Russian citizens, on the one hand, Russia is constantly strengthening citizens' right to control and be informed about their personal data. The Law on Personal Data specifies that the processing of personal data by data processors requires the consent of the personal data subject. In March 2021, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation proposed that data processors may anonymise personal data only with the consent of the personal data subject, or in other cases provided for by the law on personal data[5] . This proposal further strengthens the right of citizens to be informed about the processing of personal data. In addition, the "Right to be Forgotten" bill gives Russian citizens greater control over their personal data. "The right to be forgotten" means that citizens have the right to request search engine operators to stop sending (i.e. delete) links to information on the internet that provides access to information about them, "relevant information" being information that violates the laws of the Russian Federation, is inaccurate, does not have Information that is not relevant, is not realistic and has no significance for the subsequent activity of the citizen[6] .

On the other hand, Russia is limiting the flow of personal data of Russian citizens within and outside the country by deepening data localisation. According to the localisation act, all data concerning Russian citizens should be kept on servers within Russia's own borders. Although Russian data legislation limits the scope of application of the law by nationality, most internet companies do not pay attention to the collection of data on the nationality of their users in the course of providing their services, so in practice the law is applied equally to all users residing in the country. Furthermore, the restrictions on the flow of personal data in Russia do not mean that Russia does not allow the transfer of personal data of its citizens across its borders. For the cross-border movement of personal data, Russia has established, inter alia, a "whitelist" system under the Personal Data Act. The Act provides that no additional consent of the data subject is required for the transfer of personal data outside the country when the jurisdiction to which the personal data is transferred ensures adequate protection of the personal data. All countries that are signatories to the 108 Convention are considered to be jurisdictions that provide adequate protection for personal data. For countries that are not signatories to

ISSN 2616-7433 Vol. 4, Issue 7: 53-58, DOI: 10.25236/FSST.2022.040710

the 108 Convention, Russia may still include them in its "white list" of countries where personal data flows across borders, depending on whether the country has a comprehensive personal data protection system and whether it has a system of penalties for breaches of personal data protection laws, etc. Russia can still be included in the "white list" of countries that "provide adequate protection" for the cross-border flow of personal data. In the case of transfers of personal data to countries that "do not provide adequate protection", the data processor must obtain the written consent of the data subject or meet the conditions set out in the Personal Data Act. It should be noted that most of the countries that have signed the "108 Convention" are European countries, while China and the United States, which are major digital trading countries, are considered to be "unable to provide adequate protection".

The importance of the dual nature of the right to personal data and the right to property of citizens is determined by the fact that the right to personal data is comprehensively and fully protected in Russia, with the fundamental aim of safeguarding national security. In protecting the right to personal data, Russia has always upheld the principle of data sovereignty, i.e. the State always supervises the processing of personal data of citizens. This principle ensures the normal flow of personal data of Russian citizens within the country and also gives the State the right to determine how personal data of citizens should participate in international data flows.

2.2.3 Strict regulation of the content of circulation data

In the Internet, the social reality reflected in the data can be considered as the content of the data[7] .

Depending on the content of the data, Russia has adopted several pieces of legislation that classify data as circulating or prohibited. Data that endangers national security, obstructs the social order or violates the rights and interests of individuals falls within the scope of data that is prohibited from circulation. For example, under the Law on Mass Media, the Russian Federation prohibits the use of the mass media to disseminate information on materials that commit acts of terrorism or propagate terrorism, as well as other extremist materials that incite war, national, racial or religious hatred, or hostility.[8] In December 2021, Google was fined 1.0 million dollars for failing to remove content that the Russian internet regulator deemed "illegal for spreading extremism. In December 2021, Google was fined $170 million for failing to remove what the Russian internet regulator deemed to be "illegal content spreading extremism", the first time that Russia has fined an IT company in such a case based on the size of its local turnover. While most data with legal content can be circulated freely under the relevant laws and regulations, information relating to state secrets or other information required to be kept confidential by law, personal information of citizens and information on intellectual property rights is classified as relatively prohibited data. The Law on Mass Media, the Law on New Rules for Prominent Bloggers and the Russian Law on Access to Government Information prohibit the circulation of information that requires special confidentiality. Personal information about citizens and intellectual property rights require the authorisation of the data owner before they can be circulated.

In order to fully implement the laws and regulations enacted in the field of cyber security, the Russian Federation has established a system of Internet regulation with the Russian Security Council as the hub. In addition to the Russian Security Council, the Ministry of Telecommunications and Mass Media, the Federal Security Service and the Network and Services Association have been established. Roskomnadzor was established by Decree No. 1715 of the President of the Russian Federation in December 2008 and is responsible for regulating compliance with laws and regulations by the relevant entities. Roskomnadzor was established by Federal Presidential Decree 1715 of December 2008. Since its establishment, Roskomnadzor has imposed penalties on a number of internet companies. For example, in 2018, Roskomnadzor issued a request to the App Store and Google Play Store to take down the encrypted messaging software Telegram because it had been used to commit terrorist attacks and endanger national security. In addition to government agencies, Russia's internet regulators include certain public interest organisations, government-directed enterprises, social organisations and other non-governmental bodies. Although government agencies dominate the regulation of data security in Russia, non-governmental organisations also play an important role in maintaining data security. For example, the Alliance for a Safe Internet, a social organisation, is actively assisting state agencies in the fight against the owners of Internet resources that spread dangerous information on the Internet (such as extremism, violence, drug use, etc.) in the context of Russia's "Clean Net" campaign, and has achieved significant The results are significant. According to statistics, the proportion of child pornography on the Internet in Russia has fallen significantly and is now behind the United States and the Netherlands.

2.2.4 Increasing penalties

The Russian Federation mainly imposes fines, bans and other penalties on subjects that violate the

ISSN 2616-7433 Vol. 4, Issue 7: 53-58, DOI: 10.25236/FSST.2022.040710

Information Act, the Mass Media Act, the Personal Data Act and other laws. On the whole, the Russian regulator's regulatory work is characterised by a wide range of regulations and light penalties, but recently there has also been a trend to increase penalties for technology companies.

In December 2018, Roskomnadzor was fined 500,000 rubles by the Russian authorities for failing to comply with the legal requirement to remove banned websites from its search results, which was not a large fine for Google. In July 2019, Roskomnadzor again sampled Google's search results and found that more than a third of the links to banned information remained in the search results, resulting in a fine of 700,000 roubles being imposed on Google. Under the Information Act, as of 1 October 2018, search engines entering the Russian market must accept a catalogue of officially banned pages in Russia and block all search results within the catalogue. Violation of this provision will result in a fine of between 500,000 and 700,000 roubles. As a result, the fine imposed by Roskomnadzor on Google Inc. was raised from the minimum to the maximum from December 2018 to July 2019. In addition to this, according to the above, for the first time in Russia, a fine penalty was imposed on an IT company based on revenue due to Google's refusal to remove illegal content.

In addition to fines, Russia has taken the penalty of a Russia-wide ban on some companies that violate the relevant laws. Companies such as Linkedin, BlackBerry, Mobile Home and Connect Me have been blacklisted by Roskomnadzor for refusing to store Russian citizens' data on servers in Russia. in November 2021, Roskomnadzor named 13 foreign technology companies and required them to establish, as of 1 January 2022, an official representatives (e.g. branches, representative offices, etc.) or face possible restrictions or a full ban. According to the list, most of the companies named are American companies, such as Google, Apple and Twitter.

Despite the increasing penalties imposed on technology companies in Russia, the effectiveness of their enforcement shows that the high fines imposed on large technology companies such as Google and Twitter, which have a near monopoly in Russia, have not fundamentally restrained such companies, and data breaches have been repeated.

3. Challenges to two-way compliance for cross-border data flows involving Russian companies

3.1 Exposure to legal risks and conflicts

In recent years, Russia has continued to improve its data legislation and, as a result, companies that fail to keep abreast of and familiarise themselves with the various acts introduced by the Russian authorities are at high risk of facing severe penalties from the Russian side. For example, in May 2017, WeChat (Overseas Edition) was blacklisted and completely blocked for failing to provide Roskomnadzor with information on its business registration, server address and description of software features in the country in which it was located in a timely manner as required. In response, the head of Tencent said that the result was due to a misunderstanding of the law between the two parties.

In the area of data legislation, Russia's 'silo model' contrasts with the trend towards liberalisation of international cross-border data flows, and its differing requirements for data entry and exit from other countries, which pose a challenge for businesses in terms of data compliance. For example, as mentioned above, data processors in Russia who provide personal data of citizens outside of Russia, in addition to providing data to countries that are signatories to the 108 Convention and to the white list established by Roskomnadzor, are required to ensure that the country in which the data recipient is located is able to provide "adequate protection" for data subjects and rights. According to China's "Data Exit Security Assessment Measures (Draft for Public Comments)" promulgated in October 2021, data processors who provide personal data outside of China that should be subject to security assessment are required to declare the exit security assessment to the provincial Internet information department where they are located to ensure that the data recipient can provide security for the data. The draft law also provides for the protection of personal data. Unlike Russia, China requires a security assessment of the data recipient and does not require an assessment of the data recipient's country. In addition to China, legal conflicts also arise between Russia and countries such as the US, which strongly advocate the free flow of data.

3.2 Elevated legal costs

3.2.1 Cost of capital

The increase in legal capital costs for companies involved in Russia is reflected in two main areas:

ISSN 2616-7433 Vol. 4, Issue 7: 53-58, DOI: 10.25236/FSST.2022.040710

the fines incurred for non-compliance and the operating costs incurred to comply with the law.

According to the previous analysis, fines for non-compliance are increasing in Russia, with companies such as Google and Twitter repeatedly being fined large sums of money for failing to remove illegal content. In addition, Russian law gives citizens the right to be forgotten, the right to information and other legal rights, which indicates that companies involved in Russia are extending the period of protection of their personal data, and Russia requires network operators to keep their citizens' personal data in Russia for more than six months, to set up representative offices and servers.

Russia's strict data localisation policy, which greatly restricts the free flow of data and the freedom to use and share data, has dealt a serious blow to the ability of internet companies to innovate with technology, which rely on large amounts of data. For small technology innovators, the high cost of legal compliance forces them to invest less in technological innovation, directly affecting the very foundations of their survival. In other words, if the legal costs of complying with Russian law are much higher than the benefits they can achieve in the Russian market, companies may choose to simply withdraw from the Russian market for their own long-term development.

3.2.2 Technology costs

In the face of an increasingly challenging international situation, Russia's data localisation policy will inevitably be strengthened for the purpose of maintaining national security, which means that the country's regulation of data security will become even stricter. Companies will need to conduct rigorous self-examination of their own data collection, storage, circulation and service processes in order to cope with the increased scrutiny in the future.

4. Conclusion

In the era of big data, data has become an important tool for the development of the digital economy, but data is a double-edged sword. The rational use of data can bring a better service experience to users, but the unrestricted expansion of the free flow of data can undoubtedly cause problems such as the leakage of user privacy and even pose a threat to national security. Against the backdrop of liberalised international data flow rules, Russia has decided to adopt a "silo" model and implement a strict data localisation policy, which is not only affecting its own economic development, but is also having a significant impact on Russian businesses, especially those in the technology sector. Russian companies should address the challenges of data security governance and carefully analyse the measures they should take to achieve data compliance, so that they can turn their passivity into initiative and achieve their own stable development.

References

[1] Russian Federation Federal Law on Personal Data [EB/OL]. http://www.consultant.ru/ document/ Cons_doc_LAW_61801/

[2] He Bo. Legislative rules and enforcement practices of cross-border data flow in Russia [D]. Big Data, 2016(02).

[3] On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" and Certain Legislative Acts of the Russian Federation on the regulation of Information Exchange using Information and Telecommunications Networks (Federal Law No. 97-F3 of May 5, 2014) [EB/OL]. http://www.consultant.ru/document/cons_doc_LAW_162586/

[4] On amendments to certain legislative acts of the Russian Federation in terms of clarifying the procedure for processing personal data in information and communication networks [EB/OL]. http:// www.consultant.ru/document/cons_doc_LAW_165838/

[5] Beijing Xindalie Law Firm. New Fines and Possible New Restrictions in the Field of Personal Information Protection in Russia [EB/OL]. https:// new.qq.com/ omn /20210506/ 20210506A048SY00. html

[6] The Law of Oblivion [EB/OL]. https://new.qq.com/omn/20210506/20210506A048SY00.html

[7] Mi Tienan. Research on the Regulation of Online Data Circulation in Russia [D]. China Applied Law, 2021(01).

[8] Federal Law on Mass Media of the Russian Federation [EB/OL]. https://base.garant.ru/10164247