ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 105

1st International Scientific and Practical Conference on Digital Economy (ISCDE 2019)

Legal enforcement of import substitution in the field of digital sovereignty protection of the Russian Federation

Kolontaevskaya I.F.
Moscow Witte University
Moscow, Russia
kolont@bk.ru

Kamenskaya E.V.
Moscow Witte University
Moscow, Russia
ekamenskaya@muiv.ru

Uvarova I.A.
Moscow Witte University
Moscow, Russia
iuvarova@muiv.ru

***Abstract* — The paper determines the need for effective organizational and legal measures in the Russian Federation to stimulate import substitution in the information sphere. It is proved that the Russia's transition to the import substitution of digital products and software is caused by real threats posed by cyber dependence on foreign digital technologies. The concept of digital (informational) sovereignty, which is understood as the right of the State to independently formulate an information policy regardless of external influence, exercise control over its information environment, and ensure information security both in the national and global information space, has been revealed. The current state of the regulatory framework for import substitution processes in the information sphere has been analyzed. Unresolved issues have been developed. Concrete proposals are being made to improve the organization-legal protection of the digital sovereignty of the Russian Federation.**

Keywords — digital (informational) sovereignty, information security, import substitution, software, regulatory support, information infrastructure.

I. INTRODUCTION

Russia's transition to domestic import substitution in the field of information technology (IT) and software is of fundamental importance from the point of view of personal and public cybersecurity, national digital sovereignty as a whole. The transfer of information processes to domestic software (from *English* "software (program)") is caused by real threats posed by cyber dependence on foreign digital technologies. The virtually unlimited possibilities that telecommunication systems provide allow to freely invading various spheres of activity of countries, carrying out information aggression against countries that are not able to protect their digital sovereignty [4]. At the same time, the main threat is that in the case of a politically-motivated decision, it is possible to disable entire global services that provide vital functions in various fields. As a result, business life in the country may practically stop. Obviously, States without their own digital platforms in a changing world can lose, if not their sovereignty, then a huge number of opportunities and the right to the future [9].

II. RESEARCH METHODOLOGY

Based on the general scientific methods of cognition (the dialectical method, induction, deduction, analysis, and synthesis), the paper implements targeted and systematic approaches to determining the legal enforcement for import substitution in the field of digital sovereignty protection of the Russian Federation. A number of private scientific and special methods of cognition have been used, as follows: legal-linguistic, formal-logical and formal-legal, methods of abstracting, generalizing, analogy, and modeling.

By the results of a legal- scientific analysis of the regulatory support of import substitution processes in the field of digital sovereignty protection in the Russian Federation, proposals to improve the legal regulation of these processes have been developed.

III. RESULTS

It should be immediately noted that the concept of digital sovereignty is not defined by law. Federal Law of July 7, 2003, No. 126-FZ *On Communications* establishes the legal basis for activities in the field of communications in the territory of the Russian Federation and in the territories under the jurisdiction of the Russian Federation. Article 1 of the Law defines certain principles for ensuring the state sovereignty of Russia in the information space: creating the conditions for the development of the Russian communications infrastructure, providing centralized management of the Russian radio-frequency resource, including the orbital-frequency one, and the numbering resource; creating the conditions to ensure communication requirements for the needs of state authorities, the needs of the state defense, state security, and the rule of law.

Summarizing various points of view [7, 6, 2], digital (information) sovereignty can be defined as the right of the State to independently form an information policy regardless of external influence, exercise control over its information sphere, and ensure information security in both national and global information space. Information sovereignty includes

any components related to the information sphere of the State: technological, political, legal, economic, ideological, and social.

At present, the formation of the organization-legal basis aimed at ensuring the security of the national information infrastructure, which has become especially relevant after the introduction of sanctions against Russia from March 2014 by Western countries is underway in the Russian Federation [5]. In this regard, the issue of import substitution in the field of information technology has come to the fore.

Active steps to move towards import substitution of software were made in 2015, when the *Law on the Creation of the Register of Russian Computer Programs and Databases Restricting the Purchase of Foreign Software for Government Agencies* was adopted. The *Decree of the Government of the Russian Federation* dated November 16, 2015, No. 1236 and the *Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation* (MinComSvyaz) dated April 1, 2015, No. 96 imposed a ban on procurement for municipal and state needs of software not included in the Unified Register of Russian Programs for electronic computers and databases (hereinafter referred to as the "Registry"). At the same time, the logic of the initiative of the MinComSvyaz was that import substitution would give Russian developers and companies a real chance to conclude profitable contracts with government agencies and receive financing for business development, which, in turn, would increase the income of domestic manufacturers of digital products and increase new jobs.

Unified Register containing information about all the software officially originating from the Russian Federation began to function in January 2016 [9]. All IT solutions that entered the Register began to take priority in public procurement. As a result, the share of Russian software in government procurement is already 65% now (20% in 2015) [12].

Similar protectionist measures were taken against state-owned companies, which were also instructed to give preference to Russian digital technologies from the Register when purchasing software [11]. It is assumed that the share of Russian software purchased by state-owned companies should exceed 50% by 2021, and 70% by 2024. For government agencies, this percentage in 2024 should be 90% [1].

In addition to protectionist and restrictive measures of legal enforcement for Russian developers of digital technologies, since 2009, lower rates for insurance premiums have been introduced for IT companies.

The implementation of the state sovereignty in the information space is carried out through the information function of the state and information policy [5]. In 2016, by Decree of the President of the Russian Federation dated December 05, 2016, No. 646, the Doctrine of Information Security of the Russian Federation was approved. The national project "Digital Economy of the Russian Federation National Program" provides for the creation of "end-to-end" digital technologies mainly based on domestic developments. The Russian Federation has taken a course towards creating a global competitive infrastructure for the transmission, processing, and storage of data, as well as the functioning of digital platforms for working with data to meet the needs of citizens, business, and government based on domestic developments.

Currently, there is a large-scale dissemination and development of the Internet, mobile communications, and telecommunications network throughout the country. This was facilitated by domestic technological developments.

Now, there is its own search engine Yandex, its popular social networks VKontakte and Odnoklassniki, the largest RuNet mail of Mail.ru, Gosuslugi.ru portal, own analogues of Uber in Russia. Aurora national mobile operating system is being tested. Work is continuing on the creation of an alternative to Microsoft Office, and in the near future, the creation of the fifth generation mobile network will begin.

A purely Russian product is the Unified Biometric System, developed by Rostelecom, PJSC, and which allows you to confirm your identity by face and voice using a video camera and microphone of your own smartphone. This technological achievement was authorized by the Federal Law of December 31, 2017, No. 482-FZ *On Amending Certain Legislative Acts of the Russian Federation*, due to which a new Article 14.1 *The Use of Information Technology to Identify Citizens of the Russian Federation* has appeared in the Federal Law of July 27, 2006, No. 149-FZ *On Information, Information Technologies, and the Protection of Information*.

If 10 years ago, 27% of Russians received no more than two TV channels, often in dubious quality, in 2019, digital broadcasting coverage in Russia amounted to 98.4% of the population, which exceeds the corresponding figures in highly developed European countries [9].

On November 1, 2019, the Law came into force on ensuring the safe and stable operation of the Russian segment of the Internet in case it is disconnected from the global network infrastructure. In accordance with the Law, a duplicating infrastructure for the smooth operation of the Internet should appear in Russia. In case of threats, the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) will be able to take over the centralized management of the public communications network. The list of possible threats will be determined by the Government of the Russian Federation. The framework format of the Law assumes that its full-fledged work depends on additional by-laws and regulations, decisions of authorities and the development of information technologies.

According to K.Yu. Noskov, the Minister of Digital Development, Communications, and Mass Media of the Russian Federation, "this law is an airbag: ... if something happens, we can continue to live an ordinary life and will not lose anything" [9].

Meanwhile, import substitution processes run into serious problems. First of all, it is the uneven import substitution. If Russian companies have already taken leading positions not only in the public procurement market, but also outside the public sector in developments in the field of cybersecurity and

antiviruses, as well as electronic document management systems, then for most software classes, the results are extremely low, for example, in database development, as well as in management and design systems. At the current stage, the solution to the problem of import substitution should be stimulating the technological development of strategic sectors of the economy, the sale of expensive high-tech products in the world market that can provide the financial flows that are sufficient for the sustainable socioeconomic development of the country, as well as meeting the needs of the domestic national high-tech market [3].

There are objective reasons for limiting the demand for Russian digital products. So, owing to sanctions, Russian developers cannot offer their services to the oil and gas industry to solvent foreign customers. At the same time, the legislation allows the domestic customer to turn to foreign developers if the Russian counterpart "with the necessary functional, technical and (or) operational characteristics" does not exist. This legal clause is often used by government agencies, seeking by inertia to use familiar foreign software. In addition, some companies with state participation do not want to bear financial and organizational expenses for the import substitution program [1].

The problem is that many state information systems (SIS) work in close cooperation with foreign software—Internet Explorer browser and Windows operating system, developed by transnational corporation Microsoft. The Decree of the Government of the Russian Federation *On Centralized Procurement of Office Software* was sent to solve this problem, requiring that until 2020, the holders of all SISs should ensure their compatibility with Russian software.

A serious problem is the legal uncertainty of the concept of "Russian product" (or "domestic product"), which creates legal difficulties in determining domestic producers and, accordingly, Russian products for their subsequent entry in the Register. Due to the fact that when purchasing software by state bodies and state-owned companies, priority should be given to domestic software products, it is necessary to make appropriate amendments to the regulatory framework. Currently, Russian companies are considered to be registered in Russia, paying taxes to the Russian budget and not violating the laws of Russia. At the same time, many subsidiaries of foreign companies are registered in the Russian Federation, which are legally considered to be Russian ones, although they comply with the orders of foreign software copyright holders.

Russian developers are worried by the decision of the Expert Council on Import Substitution, which oversees the work of the Register, to phase out software based on foreign databases, application servers, and platforms. Due to the fact that no clear legal definition of platforms has been given, it remains unclear which products from the Register can be removed. As a result, customers do not want to buy domestic software, which may soon be excluded from the Register. In such a situation, customers should be given official explanations on the contents of the Register, so that they understand what domestic programs are in demand, implementation experience, and enjoy reliable support.

It is also necessary to develop adequate criteria for the inclusion of digital products in the Register. Currently, belonging to the domestic software is determined by the owner of the exclusive software rights and the ultimate beneficiary, who should be citizens of the Russian Federation. However, a Russian developer can just buy exclusive rights from a foreign company, which will automatically make the software domestic. But this does not guarantee the presence in Russia of real competencies for maintaining and developing the product.

IV. CONCLUSIONS

Participation in the import substitution program requires Russian developers to incur large costs, including the costly examination of the Russian origin of the product. Therefore, it is necessary to expand preferences and thereby help Russian companies get into the Register, increase their share of participation both in the public procurement market and in the corporate segment.

Therefore, it is necessary to improve the regulatory support of digitization processes and ensuring information security.

We can conclude that at present, the relevance of the development of digital production at the national level of each State is determined not only by the desire to improve the country's economy, but also by issues of national security and the preservation of digital sovereignty.

In the Russian Federation, there is sufficient potential to guarantee its digital sovereignty. At the same time, Russia, developing domestic digital technologies, does not set as its goal isolation from the global market. The Russian Federation will promote its developments abroad and intends to work together with international partners. The goal of the digital economy and digital development in the world is to build a single, secure digital space.

Acknowledgement

The paper was published as part of the scientific project supported by the Russian Foundation for Basic Research No. 19-011-00373.

References

[1] Aleksandrova Ye. Okhranitel'nyy soft. Naskol'ko effektivny protektsionistskiye mery po importozameshcheniyu PO// URL: https://www.kommersant.ru/doc/4125716 (data obrashcheniya 01.11.2019).

[2] Artamonov D.S. Informatsionnyy suverenitet, teoreticheskiy aspekt // Materialy VIII Mezhdunarodnogo Konstitutsionnogo Foruma, posvyashchennogo 80-letiyu Saratovskoy oblasti. – 2017. – str.16-20.

[3] Betelin V. B. O probleme importozameshcheniya i al'ternativnoy modeli ekonomicheskogo razvitiya Rossii // Strategicheskiye prioritety. — 2016. — № 1 (9). — S. 11—21.

[4] Dzhoys E.A., Simakov A.A. Tsifrovoy suverenitet i pravovoye regulirovaniye piringovykh platezhnykh sistem// Nauchnyy vestnik Omskoy akademii MVD Rossii. 2018. № 3 (70). S. 54-60.

[5] Yefremov A.A. Formirovaniye kontseptsii informatsionnogo suvereniteta gosudarstva//Pravo. Zhurnal Vysshey shkoly ekonomiki. 2017. № 1. S. 201-215.

[6] Zorina Ye. G. Informatsionnyy suverenitet sovremennogo gosudarstva i osnovnyye instrumenty yego obespecheniya // Izv. Sarat. un-ta. Nov. ser. Ser. Sotsiologiya. Politologiya. – 2017. – T. 17, vyp. 3. – S. 345–348.

[7] Kucheryavyy M. M. Gosudarstvennaya politika informatsionnogo suvereniteta Rossii v usloviyakh sovremennogo global'nogo mira // Upravlencheskoye konsul'tirovaniye. – 2014. – Vyp. 9 (69). – S. 12.;

[8] Medvedev D.A.: Tsifrovoye budushcheye uzhe sovsem ryadom// URL: https://rg.ru/2019/11/03/dmitrij-medvedev-cifrovoe-budushchee-uzhe-sovsem-riadom.html (data obrashcheniya 05.11.2019).

[9] Noskov K.YU.: «Ves' mir zaviduyet nashim tsifrovym tekhnologiyam»// https://digital.gov.ru/ru/events/39402/(data obrashcheniya 01.11.2019).

[10] Ofitsial'nyy sayt Yedinogo reyestra rossiyskikh programm dlya elektronnykh vychislitel'nykh mashin i baz dannykh https://reestr.minsvyaz.ru/(data obrashcheniya 01.11.2019).

[11] Teper' i goskompaniyam pridetsya pokupat' rossiyskiy soft v prioritetnom poryadke// https://www.vedomosti.ru/technology/articles/2016/07/18/649538-teper-goskompanii-dolzhni-pokupat-rossiiskii-soft-prioritetnom-poryadke

[12] 12. Shmyrev V. Informatsionnyye tekhnologii v gossektore// URL: https://cnews.ru/news/top/2019-04-24_dolya_rossijskogo_po_v_zakupkah_gosorganov_dostigla (data obrashcheniya 01.11.2019).