Otylia Bieniek
ORCID: 0000-0002-9098-4335
Uniwersytet Wrocławski

The specificity of the so-called digital sovereignity in Russia on the example of the Russian segment of the Internet – the RuNet

Abstract

Due to the activity of the Russian Federation in the digital information space, it seems necessary to examine the role (identity) of Russia in the sphere of international information security and the process of shaping Russian national interests in this field. One of the steps leading to the achievement of the above research objective is an attempt to analyse the specificity of the Russian segment of the Internet – the RuNet, which functions according to internal regulations and is becoming more and more independent of the global network. The main hypothesis of the article is the assumption that the nature of the Russian segment of the Internet – the RuNet, deeply embedded in the Russian culture, is an excellent space for implementing the so-called digital sovereignty, which is on a par with digital authoritarianism in Russia. In the course of these considerations, reference was made to Russia's geopolitical and cultural issues concerning the conceptualisation of Russian national interests in the changed international information space. The article briefly presents the Russian legislation related to the process of implementing the so-called digital sovereignty.

Keywords: Russian segment of the Internet – the RuNet, digital sovereignty, information security

Introduction

The current dynamic changes in socio-economic relations are the result of a digital transformation that can be compared to the Industrial Revolution in the 19th century. At that time, Europe was characterised by a rapid industrialisation process. The radical changes that took place in the so-called age of steam and electricity concerned the development of technology and the economy and gave rise to a new social formation for which the most important capital was the production of goods and services. As a result, there were also social inequalities and conflicts characteristic of the industrialisation era[1]. The expansion of the West, which paved the way for global modernisation as well as the westernisation of non-Western societies, has left its mark on the vectors of action in present-day Russia's digital information space[2].

[1] M. Xu, J.M. David, S.Kim Hi, 'The Fourth Industrial Revolution: Opportunities and Challenges', *International Journal of Financial Research* Vol. 9, No. 2, 2018, pp. 90-91, accessible at: www.researchgate.net/publication/323638914_The_Fourth_Indu

[2] J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej: między nauką, ideologicznym dyskursem a praktyką*, Gdańsk, 2010, p. 47.

On the threshold of the digital revolution, contemporary Russia again faced two main problems – one purely geopolitical, concerning the conceptualisation of Russian national interests in a changed international space, and the other – 'cultural', the essence and validity of which are the subject of Russian geopolitical disputes carried on to the present day. First of all, the polemics in the Russian scientific community regarding the issue of modernisation in Russia relates to the past and the situation of the USSR, the system of which, according to the majority, was not prepared for the advent of modern civilisation of the 'third wave' and collapsed because it was unable to solve contemporary civilisation problems. Therefore, the geopolitical discourse on contemporary challenges related to the digital revolution, according to Russian scientists, is a modern version of the 'eternal' Russian dispute over the attitude towards Western European civilisation[3].

It should be assumed that the geopolitical disputes in question concern not only Russia, but the entire modern world and all the societies that inhabit it. Russia's ambitions to isolate its own digital information space is a response to the rapid social changes taking place in the modern world, related to the IT revolution, globalisation, the revival of localisms and nationalisms, the construction of a global civilisation, the transition from an industrial to a post-industrial society, and the shaping of a network society[4]. The aspirations of states to digital sovereignty resulting from the digital revolution require new actions related to the control of the Internet. These include: introducing a new standard of decision-making and implementing political activities, planning public policies, regulating new economic phenomena, protecting digital data and privacy, creating strategies for using new technologies, developing digital infrastructure and digital competences of the society, developing innovation and science[5]. The trend in the field of regulation of new technologies, directly related to the control of the Internet, is the difference between Russia, with its repressive activities on the Internet and digital authoritarianism, and the activities of the broadly understood West, which aims at a democratic and transparent policy of data flow (EU) and their monetisation and building trusted relations with technological partners (USA), as well as building competences in the field of strategic communication (NATO)[6]. It is certain that the development of the Russian segment of the Internet – the RuNet is part of the global trend of establishing the boundaries of the Internet space and thus shaping a new (digital) order.

The aim of this article is an attempt to analyse the *specificity* of the Russian segment of the Internet – the RuNet, taking into account the influence of geopolitical and cultural aspects on the process of shaping Russian national interests in the new digital reality.

[3] Ibidem, p. 257.

[4] Ibidem, p. 315.

[5] K. Śledziewska, R. Włoch, *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa 2020, p. 246.

[6] *Raport: Geopolityka Nowych Technologii Cyfrowych*, Warszawa, 2020, p. 13-21, accessible at: https://ik.org.pl.

1. Russia in the new (digital) order

Leading international actors – states, international organisations and corporations – are moving away from the idea of a free flow of data between national and regional borders. This means that access to the Internet and certain digital content is governed by local laws. Therefore, in the research discourse on digital sovereignty, the term 'Cyber Westphalia' is applied, which is used by international lawyers, political scientists and security specialists. On the other hand, geographers use the term 'Balkanisation of the Internet', 'Splinternet', which indicates a tendency to recreate physical borders between countries in the case of the Internet. In a broader sense, it is the totality of phenomena leading to the demarcation of the global network, an increase in control over Internet content and network infrastructure[7]. The above shows that the digital revolution, instead of the utopia of the network society, brought about a capitalist regime of digital platforms, to the expansion of which some (developed) countries and international organisations began to respond. Due to growing regional and political influence, fragmentation of the Internet has become a direct consequence of states' efforts to maintain their own identity in the digital information space. Using the benefits of digitisation to an increasing extent, depending on the standards set by a given state, international organisation or corporation, is associated with the loss of users' privacy and their surveillance[8]. According to Prof. Shoshana Zuboff, a social psychologist at Harvard University and author of the book *Age of Surveillance Capitalism*, surveillance is the backbone of the digital economy, and our data is its main raw material[9]. It should be emphasised that despite the fact that global technology giants build their power thanks to the collection and processing of digital data, it is states and their institutions that own significant information resources[10].

Another term – 'digital sovereignty' has gained in popularity in recent years. This is due to the efforts of leading countries to increase their own technological capabilities and acquire the ability to set rules and create value in a world centred around new technologies. On the one hand, the sovereign needs the state to control borders more effectively and protect a citizen from the negative consequences of globalisation. At the same time, they also want to have full and unfettered access to information, without which they are unable to make informed political choices and control the executive power. On the other hand, there is a noticeable tendency to define sovereignty as an expression of the will of rulers, and not

[7] A. Bógdał-Brzezińska, J. A. Wendt, *Geopolityczny kontekst suwerenności informacyjnej Rosji w cyberprzestrzeni i jej znaczenie dla bezpieczeństwa międzynarodowego*, Siedlce, 2020, p. 104.

[8] Cf. [in:] Jan J. Zygmuntowski, *Kapitalizm sieci*, Warszawa 2020.

[9] https://www.pap.pl/aktualnosci/news%2C1160253%2Cprof-shoshana-zuboff-inwigilacja-jest-podstawa-gospodarki-cyfrowej-nasze.

[10] *Raport: Geopolityka Nowych Technologii Cyfrowych*, Warszawa, 2020, p. 67, accessible at: https://ik.org.pl.

of the nation, i.e., the sovereign. Paradoxically, digital sovereignty is becoming the subject of a dispute in the form of the government's struggle for full control over information[11].

Based on the results of 80 expert interviews with Russian representatives of sectors such as: education and science (51%), information technology (28%), state and local government administration (23%) and business (15%), as well as 10 discussions within civic society in focus groups involving young people (over 70 people aged 21-27), Russian scientists from Tomsk State University made an attempt to analyse the process of implementing digital sovereignty in Russia[12].

The vast majority of the respondents (83.3%) confirmed the relevance of the problem of digital sovereignty in Russia (9-10 points on a 10-point scale). Firstly, it was indicated that most of the key areas of human life are gradually being transferred to the digital space, which makes the traditional aspects of sovereignty less important and is replaced by new areas covered by digitisation, i.e.: education (38.9% of responses), state and (less frequently) local government administration (33.3%), economy (especially banking sector – 22.5%). In addition, the high level of digitisation in Russia has been noted by representatives of the business environment in the field of logistics and transport, as well as public safety and medicine. The vast majority of specialists highlighted the impact of digital transformation on different levels of communication[13].

Some Russian specialists taking into account global communication enabled by digital extraterritoriality are sceptical about the successful implementation of the so-called digital sovereignty. The remaining (larger) part expresses optimism towards state management of digital resources that function in the domestic (Russian) segments of the Internet. Therefore, most of the respondents support the regulation, supervision and control of the activities of digital platforms and the possibility of blocking published information by Russian authorised bodies and state organisations[14].

Russian experts associate the popularity of the phenomenon of digital sovereignty, firstly, with the presence of a significant number of external global actors using the Russian digital space for their own interests, and secondly, with the problem of the lack of systemic legal regulations in this area in Russia. 'The problem of developing a theory, without which it is difficult to create doctrinal foundations, has not been solved. In the (Russian) public

[11] M. Zaborowski, *Bitwa o suwerenność*, Warszawa 2019, accessible at: https://publica.pl/teksty/zaborowski-bitwa-o-suwerennosc-66438.html.

[12] В.А. Никонов, А.С. Воронов, В.А. Сажина, С.В. Володенков, М.В. Рыбакова, *ЦИФРОВОЙ СУВЕРЕНИТЕТ СОВРЕМЕННОГО ГОСУДАРСТВА: СОДЕРЖАНИЕ И СТРУКТУРНЫЕ КОМПОНЕНТЫ (ПО МАТЕРИАЛАМ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ)* Исследование выполнено при финансовой поддержке РФФИ и ЭИСИ, Томск 2021, p. 207.

[13] Ibidem, p. 208.

[14] В.А. Никонов, А.С. Воронов, В.А. Сажина, С.В. Володенков, М.В. Рыбакова ЦИФРОВОЙ СУВЕРЕНИТЕТ […], Томск 2021, p. 207.

sector, there is no ordering of definitions such as: automation, computerisation, digitisation, which causes mixing of concepts, which are often confused'[15].

Based on the expert interviews conducted, Russian scientists from Tomsk State University described digital sovereignty in Russia as the state's ability to independently determine the degree and mode of participating or not participating in relations concerning the use of digital technologies to pursue its own interests. At the same time, the process of implementing sovereignty into national segments of the digital space should be regulated by national legislation in the interest of a particular state[16].

The concept of digital sovereignty in Russia was also explained by the representative of the Eurasian Economic Union, T. Sarkisian. According to him, it means the independence of the state in managing digital transformation and the creation of a new ecosystem that excludes the possibility of external influence on its functioning and stability[17].

The main doctrinaire of the Russian concept of digital sovereignty is I.S. Ashmanov, Chief Executive Officer of the company Ashmanov and Partners, dealing with internet marketing in Russia. According to him, digital sovereignty is the right of the state to define its information policy and to manage its infrastructure, resources, information security etc. In Ashmanov's opinion, digital sovereignty can be divided into several categories. One of them is electronic sovereignty, which is related to protection against cyber attacks. Thus, the concept of the definition of Ashmanov's digital sovereignty is identical to the concept of information sovereignty, which began to appear in Russian state documents from 2016[18].

It can be assumed that Europe has also been operating in the area of the so-called digital sovereignty in recent years. This is evidenced by the Digital Services Act (DSA, a code of digital services), which regulates matters related to content moderation, targeted advertising and the use of algorithms to recommend content, and the Digital Markets Act (DMA, a code of digital markets), which in turn imposes a number of additional obligations on the largest platforms and directly prohibits many of the unfair practices that platforms currently apply to their users and business customers. In addition, the General Data Protection Regulation (GDPR) has been in force in Europe for several years[19].

---

[15] Ibidem, p. 208.

[16] В.А. Никонов, А.С. Воронов, В.А. Сажина, С.В. Володенков, М.В. Рыбакова ЦИФРОВОЙ СУВЕРЕНИТЕТ […], Томск 2021, p. 210.

[17] Т. САРКИСЯН, Цифровой суверенитет и цифровая повестка ЕАЭС, Россия в глобальной политике, 2021, accessible at: www.globalaffairs.ru/articles/czifrovoj-suverenitet-eaes.

[18] Бухарин В.В., КОМПОНЕНТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ КАК ТЕХНИЧЕСКАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, Москва 2016, p. 77, accessible at: www. cyberleninka.ru.

[19] *Cyfrowa przyszłość Europy*, accessible at: https://www.consilium.europa.eu/pl/policies/a-digital-future-for-europe/.

Digital sovereignty has also been defined by the firm Ovhcloud, the European leader among cloud service providers, as the state's ability to control all digital assets, from the economic, social, and political point of view, without the involvement of third parties or external influence. The foundation is freedom of choice and independence from infrastructures, platforms and Internet access points located outside Europe[20].

It is worth noting that an expert coalition of the so-called Polish Charter of Digital Sovereignty, led by the Instrat think-tank, is working on a basic set of rules that will enable a sustainable and socially beneficial development of the digital economy in Poland[21]. A report prepared by Instrat shows that, in a broad sense, the concept of digital sovereignty means the ability of states and users themselves to exercise their rights and shape the digital economy in line with their social and development needs[22].

In the context of the growing importance of the so-called digital sovereignty of states resulting from the inclusion of activities related to the control of the Internet in national security policy, the main threat is favouring developed countries and deepening the problem of economic underdevelopment of developing and underdeveloped countries, exacerbating the existing inequalities[23].

2. The specificity of the Russian segment of the Internet – the RuNet

Contemporary Russia, in the conditions of the new digital order, as in the period of the political transformation, aims to define its own national identity and build a cultural space[24]. It can be assumed that, being beyond the reach of the development and modernisation possibilities that Europe had at its disposal, supported by the United States in the aforementioned period of the Industrial Revolution, Russia stuck in the conviction of its own distinctiveness and uniqueness to this day. The reason then was the radical attitude of the USSR leaders and the Cold War world. Then, the effect of this country's economic backwardness after the collapse of the USSR turned out to be permanent isolationism and a manifestation of a return to its sources, and the syndrome of a besieged fortress. Russia, disappointed with past processes of modernisation and westernisation, is constantly looking for development paths alternative to the West, promoting anti-Western and isolationist

[20] Cf. [in:] *Suwerenność danych w chmurze: wyzwanie dla wszystkich w całej Europie*, accessible at: www.ovhcloud.com.

[21] Cf. [in:] *Polska Karta Suwerenności Cyfrowej*, accessible at: www.cyfrowasuwerennosc.pl/o-nas/

[22] *Raport: Geopolityka Nowych Technologii Cyfrowych*, Warszawa, 2020, accessible at: https://ik.org.pl.

[23] Report of the World Economic Forum, in which the authors mainly raise the topic of the Fourth Industrial Revolution. World Economic Forum, Our Mission, accessible at: https://www.weforum.org/about/world-economic-forum.

[24] A. Epifanova, *Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet*, (DGAP Analysis, 2). Berlin 2020, accessible at: www.nbn-resolving.org/urn:nbn:de:0168-ssoar-66221-82020.

sentiments. In opposition to the Atlantists, described in the Russian geopolitical discourse as supporters of Russia's integration with the Western world, who believed that Russia should ally itself with the European Union and the United States by imitating their development model, there was a resurgence of interest in Eurasianism, and with it the rehabilitation of Asia in the Russian consciousness. Hence, the domination of the image of Russia-Eurasia in the contemporary discourse on Russia's geopolitical strategy. The above directly relates to Russia's ambitious efforts to build its own digital sovereignty. It seems that in this context, the basis of the determinants of the Russian information security system is the Russia-Eurasia perspective as an alternative to the Russia-Europe perspective. Therefore, it can be assumed that the idea of Eurasianism, referring to the belief rooted in Russian culture that Russia is neither the East nor the West, but something third, specific, constitutes the basis for the concept of building the RuNet[25].

The discussion about the extent to which the digital revolution and with it new technologies related to social communication influence the shape of political, economic, cultural and military processes was triggered by the revolutionary events of 2010-2012 taking place in the Arab world (the 'Arab Spring'), in European countries (Spain), as well as in Russia (social protests against the results of the presidential and parliamentary elections)[26]. Demonstrations organised via social media such as Facebook, toppled some hitherto irremovable dictators. A similar effect of the association of societies in the Internet space was the outbreak of multi-million protests after the rigged elections to the Duma (protests in Bolotnaya Square in Moscow)[27].

As a result, Russia started to treat the Internet as a threat and in 2012 launched a systemic offensive against freedom of speech on the Internet, the right of access to information and the right to secrecy of correspondence. Despite the fact that from the beginning of its existence, the RuNet remained the object of keen interest of special services (e.g. through the surveillance of e-mail users by the Federal Security Service thanks to the SORM-2 and SORM-3 systems), for many years no institutionalised attempts were made on a larger scale to censure it[28]. When in 2014 Putin recognised it as a 'CIA project' and called on the largest Russian Internet corporations such as Yandex and VKontakte to transfer servers to Russia[29],

[25] J. Potulski, op. cit., pp. 116-117.

[26] A. Drewniak, *Glokalność w globalnej sieci. Analiza zjawiska sieciowej tożsamości narodowej na przykładzie RuNetu*, „Człowiek i Społeczeństwo" 2015, t. 40, p. 104.

[27] D. Al-Temimi, *Federacja Rosyjska wobec Arabskiej Wiosny*, Kraków 2012, pp. 299-300, accessible at: https://repozytorium.ka.edu.pl/.

[28] M. Domańska, *Zakneblować Runet, uciszyć społeczeństwo. Kremlowskie ambicje „suwerenizacji" Internetu*, Warszawa 2021, accessible at: www.osw.waw.pl.

[29] Путин назвал Интернет проектом спецслужб США и призвал «ВКонтакте» и «Яндекс» перенести серверы в Россию, accessible at: https://www.digger.ru/news/putin-nazval-internet-proektom-specsluzhbssha-i-prizval-vkontakte-i-yandeks-perenesti-servery-v-rossiyu?ysclid=l5fel2j3pp959762821.

representatives of the Russian authorities began to explicitly define the Internet as a field of information warfare or psychological warfare, constituting an extension or an alternative to military actions. The above is justified in numerous studies by Professor Igor Panarin, who in the book *Information World War II: War against Russia* argued that all the so-called colour revolutions within the area of the Commonwealth of Independent States, as well as the 'Arab Spring' were the product of the social control technology and information aggression of the United States. Moreover, Professor Panarin distinguishes two great waves of informational aggression against 'Russia-Rus': the first, which began with perestroika, ended with the collapse of the USSR; the second, carried out from the beginning of this millennium, was to last, in his opinion, until 2020 and end with the victory of the Good (read: the Russian Eurasian idea)[30].

Currently, the image of the bipolar world dominated by the United States and China is emerging from the map of digital economy[31]. It is important that both countries represent different value systems, which, in a simplified manner, can be reduced to different civilisations: the West perceived through the prism of military power, legal achievements, ethical principles, values such as democracy or free trade, and Confucianism, which is primarily characterised by hierarchy of relations and traditional conservatism. These systems determine solutions that the world powers that build not only hard but also soft power have to offer to the world and other countries[32].

Russia conducts the process of sovereignisation of the RuNet, as it is commonly accepted[33], following the example of China, which has been isolated by the Great Firewall since 2002. The legal and technical foundations, as well as the systemic construction of the so-called sovereign segment of the Russian Internet, also resemble a national Internet launched in 2000, the so-called Kwangmyong in North Korea, or Iran's National Information Network established in 2011 (also referred to as a national intranet and a halal Internet)[34].

According to the Russian doctrine, the so-called sovereign RuNet is to serve Russia in order to defend itself against Western interference and to protect data and information created on digital platforms by its own citizens in the name of traditional Russian spiritual and moral values and compliance with the resulting rules of behaviour while using information and communications technologies. However, the formal rationale for these actions has little to do with its real goals. Russia is, firstly, intensifying its efforts to bring the Internet under strict control of secret services and law enforcement agencies,

[30] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej Operacja krymska - studium przypadku*, Warszawa 2021, accessible at: www.osw.waw.pl, p. 15.

[31] Raport: Geopolityka Nowych Technologii Cyfrowych. Warszawa, 2020, p. 32, accessible at: https://ik.org.pl.

[32] K. Gruszko, *Rola i miejsce Chin oraz USA w nowym ładzie globalnym*, Kielce 2020, p. 152.

[33] Ibidem.

[34] Ibidem.

and secondly, the Kremlin is multiplying preventive and repressive legal mechanisms and manifesting its activities through illegal practices against freedom of expression, the secrecy of correspondence and pluralism of information[35].

Russian reactions to the changing information security environment are deeply embedded in the native culture and therefore are often treated as peculiarly Russian[36]. The current political model in Russia, based on the strong role of the state, centralisation of the decision-making process, corruption and the dominant position of the power structures, also determines the course of the digitisation process. The digitisation of the Russian economy has become one of the government's priorities for the fourth term in office of President Vladimir Putin[37]. The most important instruments of Russian state policy in the field of the Internet include content filtering by Internet services and blocking network addresses by communication operators. The leading bodies responsible for the so-called sovereignty of the Russian segment of the Internet are: among the law enforcement agencies – the Federal Security Service (also the Ministry of the Interior, the Investigative Committee and the Prosecutor General's Office), and among the civilian ones – The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). In addition to state institutions, in the fight for a safe RuNet for the government, censorship pseudo-NGOs are used, created and financed by the authorities, fighting 'at grass-roots level' against dissident content. They include, among others: the Safe Internet League[38].

The following dynamic legislative actions concerning the regulation of the Internet area in Russia, supporting the introduction of the so-called digital sovereignty, are mainly based on documents such as: the Doctrine of Information Security of the Russian Federation of 2016, the National Security Strategy of the Russian Federation of 2021, the Military Doctrine of the Russian Federation of 2014, the Conceptual Views on the Activity of the Russian Federation Armed Forces in the Information Space of 2011. Important in this context is the document approved in 2021: the Basic Principles of the Russian Federation State Policy on International Information Security[39]. Amendments to the vast majority of Russian legal acts show that the digitisation process is subordinated to security issues. Some of them are:

1. 2012 – an amendment to the Law on Information, Information Technology and Information Protection: Roskomnadzor obtains the right to block websites.

[35] M. Domańska, *Zakneblować Runet…*, op. cit.

[36] J. Potulski, op. cit., p. 315.

[37] *Raport OSW: Cyfryzacja w pagonach: rozwój sieci mobilnej 5G w Rosji*, I. Wiśniewska, Warszawa 2020, p. 5. accessible at: www.osw.waw.pl.

[38] M. Domańska, *Zakneblować Runet…*, op. cit.

[39] Cf. [in:] Совет Безопасности Российской Федерации, accessible at: http://www.scrf.gov.ru/security/information/.

2. 2013 – amendment to the penal code: punishments for offending religious feelings publicly (up to three years imprisonment), in response to the happening of the Pussy Riot group at the Moscow cathedral.
3. 2013 – an amendment to the Law on Information, Information Technology and Information Protection (the so-called ‚Lugovoi Law'): the extension of the definition of extremism, Roskomnadzor takes actions at the request of the Prosecutor General's Office.
4. 2014 – an amendment to the Data Localisation Law: the law obliges legal entities to store personal data of citizens of the Russian Federation only on the territory of Russia. Its purpose was to facilitate the access of secret services to citizens' personal data, and it severely limited the possibility of using foreign servers for the purposes of activities independent of the authorities.
5. 2014/16 – an amendment to the Law on Mass Media: limiting the share of foreign capital in Russian media to 20% and introducing a ban on establishing mass media organisations in Russia by foreigners. Its purpose was to liquidate or take political control over popular media critical of the Kremlin's policy.
6. 2016 – an amendment to the provisions on terrorism and an amendment to the penal code (the so-called 'Yarovaya's package of laws'): amendments and dozens of laws that extend the powers of the state, increase control over the country's inhabitants and limit the rights guaranteed to citizens by the constitution, the possibility of depriving Russians of citizenship, prohibiting those convicted of 'wrong' posts on social networks from leaving the country, access of services to all telephone calls and electronic correspondence of citizens.
7. 2017 – an amendment to the Law on Information, Information Technology and Information Protection (the so-called 'Anonymizers Law'): a ban imposed on operators of anonymizing services (VPN, proxy servers, TOR).
8. 2017 – an amendment to the Law on Information […] abolishing the anonymity of instant messaging users and forcing registration using a subscriber number.
9. 2017 – an amendment to the Law on Information […]: granting foreign media the status of a 'foreign agent', enabling the blocking of the so-called 'undesirable organisations'.
10. 2018 – an amendment to the so-called 'Yarovaya's package of laws': an order for communication operators and owners of Internet resources to store content for a period of 6 months and to make data available to special services without a court order, the obligation to disclose encryption keys to instant messengers at the request of the Federal Security Sevice (FSB); the entry into force coincided with the 2018 FIFA World Cup Russia.

11. 2019 – an amendment to the Law on Information […] (the so-called sovereign Internet law): prohibition of disseminating 'fake news', penalties for disseminating information in a form that 'offends public morality and human dignity, expresses disrespect towards society, the state, the state symbols, the constitution or bodies exercising state power in the Russian Federation'.
12. 2020 – rapid constitutional reform aimed at strengthening the legitimacy of the regime in the eyes of the society through constitutional guarantees of social benefits, ideological accents, as well as 'sovereignisation' of Russia's attitude to international law.
13. 2021 – tightening of regulations on 'foreign agents', abolishing freedom of assembly and strengthening censorship on the Internet, restrictions and repressions against NGOs, slowing down Twitter by Roskomnadzor in response to refusal to remove 'illegal' content (largely political), removal of 'Navalny!' voting app from their online stores by Google and Apple during parliamentary elections.
14. 2022 – an amendment to the Law on Information […] (the so-called fake news law): depriving instant messaging users of anonymity by forcing registration with a subscriber number, 15 years in prison for anyone who publishes 'false information' about the Russian armed forces, new regulations intended to be a tool 'in the information war with the West in relation to the conflict in Ukraine', from 25 February 2022, preventing Russian citizens from contacting the outside world by blocking, inter alia, access to Facebook and Twitter. Therefore, Facebook, YouTube and TikTok limit access to Russian state media to fight Kremlin propaganda and disinformation[40].

The so-called Russian digital sovereignty means not so much autonomy from abroad, but full power exercised on its own territory. The example of Russia clearly shows that the modern sovereignty of the digital information space largely depends on the level of traditional state sovereignty and that the sovereign Internet model is attractive to authoritarian regimes. In addition, it is evidenced by the fact that the Russian RuNet is constructed in complete opposition to the European Convention on Human Rights and the GDPR.

[40] Based upon: B. Gołąbek, *Pierwsze lata Internetu w Rosji. Nowe medium i nowe możliwości na przestrzeni postradzieckiej*, [in:] *Rozpad ZSRR i jego konsekwencje dla Europy i świata*, cz. 1: Federacja Rosyjska, ed. A. Jach, Kraków 2011; M. Domańska, *Zakneblować Runet*…, op. cit.; eadem, *Rosja 2021: konsolidacja dyktatury*, Warszawa 2021, accessible at: www.osw.waw.pl, Komentarze OSW, eadem, M. Menkiszak, J. Rogoża, I. Wiśniewska, *Sytuacja polityczna, społeczna i gospodarcza. Rosja u progu 2021 roku*, Warszawa 2021, accessible at: www.osw.waw.pl, Федеральный закон от 27.07.2006 г. № 149-ФЗ, accessible at: http://government.ru/docs/all/98199/.

Summary

The Internet has evolved from the early stage of development of free, uncensored technology, ensuring a free way of communicating and sharing opinions and knowledge, to the next phase of development of the medium allowing for recording and analysing recorded information. Some developed countries and international organisations are developing digital sovereignty through the prism of international law by considering issues such as intervention, the use of force, due diligence and state responsibility. However, the relationship between data and territoriality challenges some of the most basic principles of the international legal order. Instead of territorial boundaries and physical ownership, new concerns relate to data access and technical capabilities. Hence, digital sovereignty and jurisdiction are not exclusive to states[41]. Therefore, it can be assumed that the Internet has become one of the areas of competition between leading countries, international organisations and corporations, which poses a challenge to international politics and security.

In accordance with the aim of the article presented in the introduction, on the basis of the analysis carried out, it can be concluded that Russia, as an actor on the international political scene, implements the so-called digital sovereignty into information security policy in accordance with geopolitical and cultural factors determining its position. The global trend of sovereignisation of the Internet, in which leading countries and international organisations take part, may deepen the role of information as a combat tool, contribute to recognising the fragmentation of the global Internet as an acceptable and natural phenomenon, and perpetuate the habits of states in the scope of isolating their own societies from the rest of the world[42]. It can therefore be predicted that the pursuit of digital sovereignty by the leading participants in international relations will become a common type of geopolitical interactions.

Bibliography

1. Al-Temimi D., *Federacja Rosyjska wobec Arabskiej Wiosny*, Kraków 2012, accessible at: https://repozytorium.ka.edu.pl/.
2. Bógdał-Brzezińska A., Wendt J. A., *Geopolityczny kontekst suwerenności informacyjnej Rosji w cyberprzestrzeni i jej znaczenie dla bezpieczeństwa międzynarodowego*, Siedlce 2020, accessible at: https://www.researchgate.net.
3. Darczewska J., *Anatomia rosyjskiej wojny informacyjnej Operacja krymska – studium przypadku*, Warszawa 2021, accessible at: www.osw.waw.pl.
4. Domańska M., *Rosja 2021: konsolidacja dyktatury*, Warszawa 2021, accessible at: www.osw.waw.pl.

[41] A. Leiter, *Cyber Sovereignty - A Snapshot from a Field in Motion*, accessible at: www.harvardilj.org.

[42] M. Ristolainen, *„Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West",* 2017, p. 124.

5. Domańska M., *Zakneblować Runet, uciszyć społeczeństwo. Kremlowskie ambicje „suwerenizacji" Internetu*, Warszawa 2021, accessible at: www.osw.waw.pl.
6. Drewniak Anna, *Glokalność w globalnej sieci. Analiza zjawiska sieciowej tożsamości narodowej na przykładzie RuNetu*, [w:] *Człowiek i Społeczeństwo*, t. 40, Poznań 2015, pp. 103-118.
7. Epifanova A., *Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet*, (DGAP Analysis, 2). Berlin 2020, accessible at: www.nbn-resolving.org/urn:nbn:de:0168-ssoar-66221-82020.
8. Gołąbek B., *Pierwsze lata Internetu w Rosji. Nowe medium i nowe możliwości na przestrzeni postradzieckiej* [in:] *Rozpad ZSRR i jego konsekwencje dla Europy i świata*, cz. 1: *Federacja Rosyjska*, ed. A. Jach, Kraków 2011.
9. Gruszko K., *Rola i miejsce Chin oraz USA w nowym ładzie globalnym*, Kielce 2020.
10. Komentarze OSW, Domańska M., Menkiszak M., Rogoża J., Wiśniewska I., Sytuacja polityczna, społeczna i gospodarcza. Rosja u progu 2021 roku, Warszawa 2021, accessible at: www.osw.waw.pl.
11. Leiter A., *Cyber Sovereignty – A Snapshot from a Field in Motion*, accessible at: www.harvardilj.org.
12. Potulski J., *Współczesne kierunki rosyjskiej myśli geopolitycznej: między nauką, ideologicznym dyskursem a praktyką*, Gdańsk, 2010.
13. Radomska E., *Poziom rozwoju gospodarki cyfrowej i społeczeństwa cyfrowego w Federacji Rosyjskiej – główne trendy i wyzwania*, Kraków 2021.
14. *Raport: Geopolityka Nowych Technologii Cyfrowych*. Warszawa, 2020, accessible at: https://ik.org.pl.
15. *Raport OSW: Cyfryzacja w pagonach: rozwój sieci mobilnej 5G w Rosji*, I. Wiśniewska, Warszawa 2020, accessible at: www.osw.waw.pl.
16. *Raport Instrat: Polska suwerenna cyfrowo. Regulacje na rzecz sprawiedliwej i konkurencyjnej gospodarki cyfrowej*, eds. B. Wawrzyniak, J. J. Zygmuntowski, F. Lamański, Warszawa 2020, accessible at: www.instrat.pl.
17. Ristolainen M., *Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West*, 2017.
18. Śledziewska K., Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa 2020.
19. Zaborowski M., *Bitwa o suwerenność*, Warszawa 2019, accessible at: www.publica.pl.
20. Zygmuntowski J. J., *Kapitalizm sieci*, Warszawa 2020.
21. Xu M., David J. M., Kim S. Hi, *The Fourth Industrial Revolution: Opportunities and Challenges*, "International Journal of Financial Research" 2018, Vol. 9, No. 2, pp. 90-91, accessible at: www.researchgate.net/publication/323638914_The_Fourth_Indu.
22. Бухарин В. В., *КОМПОНЕНТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ КАК ТЕХНИЧЕСКАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*, Москва 2016, accessible at: www. cyberleninka.ru.
23. Никонов В. А., Воронов А. С., Сажина В. А., Володенков С. В., Рыбакова М. В., *ЦИФРОВОЙ СУВЕРЕНИТЕТ СОВРЕМЕННОГО ГОСУДАРСТВА: СОДЕРЖАНИЕ И СТРУКТУРНЫЕ КОМПОНЕНТЫ (ПО МАТЕРИАЛАМ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ)*, Исследование выполнено при финансовой поддержке РФФИ и ЭИСИ, Томск 2021, accessible at: www.cyberleninka.ru.
24. *САРКИСЯН ТИГРАН*, Цифровой суверенитет и цифровая повестка ЕАЭС, Россия в глобальной политике, 2021 г., accessible at: www.globalaffairs.ru/articles/czifrovoj-suverenitet-eaes.
25. *Cyfrowa przyszłość Europy*, accessible at: https://www.consilium.europa.eu/pl/policies/a-digital-future-for-europe/.
26. *Совет Безопасности Российской Федерации*, accessible at: http://www.scrf.gov.ru/security/information/
27. Федеральный закон от 27.07.2006 г. № 149-ФЗ, accessible: http://government.ru/docs/all/98199/

Specyfika tzw. suwerenności cyfrowej w Rosji na przykładzie rosyjskiego segmentu Internetu – RuNet

Abstract

Ze względu na aktywność Federacji Rosyjskiej w cyfrowej przestrzeni informacyjnej konieczne wydaje się zbadanie roli (tożsamości) Rosji w sferze międzynarodowego bezpieczeństwa informacyjnego oraz procesu kształtowania rosyjskich interesów narodowych w tej dziedzinie. Jednym z kroków prowadzących do realizacji powyższego celu badawczego jest próba analizy specyfiki rosyjskiego segmentu Internetu – RuNet, który funkcjonuje na podstawie wewnętrznych regulacji i coraz bardziej uniezależnia się od globalnej sieci. Główną hipotezą artykułu jest założenie, że charakter rosyjskiego segmentu Internetu – RuNet, głęboko zakorzeniony w rosyjskiej kulturze, jest doskonałą przestrzenią do realizacji tzw. Autorytaryzm w Rosji. W toku niniejszych rozważań odniesiono się do geopolitycznych i kulturowych zagadnień Rosji dotyczących konceptualizacji rosyjskich interesów narodowych w zmienionej międzynarodowej przestrzeni informacyjnej. W artykule pokrótce przedstawiono ustawodawstwo rosyjskie związane z procesem wdrażania tzw. suwerenności cyfrowej.

Słowa kluczowe: rosyjski segment Internetu – RuNet, suwerenność cyfrowa, bezpieczeństwo informacyjne