Pre-print version of Martynova E. and Shcherbovich A. Digital transformation in Russia: Turning from a service model to ensuring technological sovereignty. Computer Law & Security Review. Special issue on Digital Transformation in the BRICS Countries, https://doi.org/10.1016/j.clsr.2024.106075

Digital transformation in Russia: Turning from a service model to ensuring technological sovereignty

Ekaterina Martynova and Andrey Shcherbovich

Abstract

The paper outlines core aspects of the digital transformation process in Russia since the early 2000s, as well as recent legislative initiatives and practices at the federal level. It considers the digitalization of public services, efforts towards 'sovereignization' of the Russian segment of the Internet, and the current focus on cybersecurity and the development of artificial intelligence. The paper highlights the tendency to strengthen the factor of protection of state interests and national security alongside control over online activities of citizens in comparison with the initial understanding of digital transformation as a human-oriented process aimed at increasing the accessibility and convenience of public services. It can be assumed that this change in the goals and methods of digital transformation is one of the manifestations of a broader political, social and cultural process of separation, primarily from the West, that Russian society is currently undergoing, amidst a growing official narrative of threats from both external and internal forces that require greater independence and increased vigilance, including in the digital domain.

Keywords: e-government, digital sovereignty, 'sovereign RuNet', cybersecurity, artificial intelligence

Introduction

Russia represents a significant part of the global Internet, with advanced connectivity infrastructure and high penetration of access among its population conditioning, along with low prices for communication services, active online civil society. Russia today ranks number six among countries with the highest number of the Internet users with 92.2 % Russians connected to the global network[1] which makes it one of the leaders in the Internet coverage worldwide. During 2012–2022, the volume of the Internet traffic in Russia increased more than 11 times – from 11.1 to 123.7 EB (an average growth of 27% per year).[2] By the beginning of 2023, the total number of connected Internet of Things (IoT) devices in the country reached 70.1 million units (excluding wearable devices).[3]

[1] International Telecommunication Union, Russian Federation. Individuals using the Internet. https://datahub.itu.int/data/?e=RUS&c=701&i=11624 (accessed 25 September 2024).

[2] Strategy for the Development of the Russian Communications Industry until 2035. https://digital.gov.ru/ru/documents/9120/?utm_referrer=https%3a%2f%2fwww.google.com%2f (accessed 25 November 2023).

[3] ibid.

Digitalization of the economy and public services has been a priority strategic goal for the Russian government from the early 2000s. This path, however, has been and continues to be thorny and largely determined by the broader context of political, social, economic and cultural changes that Russia has been going through over the past quarter century. The conservative turn in domestic and foreign policy during the third presidential term of Vladimir Putin (2012-2018),[4] the crisis associated with the COVID-19 pandemic and the sanctions tsunami after the start of the special military operation in Ukraine in February 2022 largely influenced the government's views on the goals and methods of digital transformation, IT regulatory policy and interaction with companies, citizens and civil society institutions in the digital domain. In this regard, this paper aims to describe the shift in the digital transformation process in Russia from a human-oriented approach that was adopted at the dawn of digitalization to the state-centric one that is has become today.

The ongoing digital transformation process in Russia is truly multi-faceted: national policies, strategies and regulations (often developed in isolation by different agencies and overlapping or even contradicting each other) are designed to promote and support the adoption of digital technologies in various sectors, including public administration, politics and the legal system, the economy, healthcare and education.[5] This paper does not attempt to analyse all existing policies and regulations. Instead, it focuses on certain areas where the paradigm shift in the digitalization process is particularly pronounced, and broadly groups them into three clusters. First, it examines the government digital transformation in Russia, that is, the stages at which public services are being digitised, datified and algorithmized. Second, it addresses the efforts to 'sovereignize' the Russian segment of the Internet. Finally, it examines the issues of cybersecurity (or, in the tradition of Russian terminology, 'information security') and the initiatives emerging on AI governance, which is becoming increasingly important for civil and military applications. Methodology of this paper is informed, first, by the 'expository' tradition in legal research, contemplating study of legal texts, including federal laws and national strategies on digital economy, cybersecurity and AI development. The black-letter law analysis is accompanied by reference to commentary in the academic literature and other sources, including assessments in the media of the successes and setbacks of the digital transformation process in Russia. Finally, to

[4] F. Lukyanov, Conservative Turn [*Konservativnyj povorot*] (in Russian), Russia in Global Affairs (19 December 2013). https://globalaffairs.ru/articles/konservativnyj-povorot (accessed 7 September 2024); A. Melville, How the Conservative Turn in Russia Relates to Conservatism in Europe and the United States [*Kak konservativnyj povorot v Rossii sootnositsja s konservatizmom v Evrope i SShA*] (in Russian), Russian International Affairs Council (11 October 2018). https://russiancouncil.ru/analytics-and-comments/comments/kak-konservativnyy-povorot-v-rossii-sootnositsya-s-konservatizmom-v-evrope-i-ssha/ (accessed 7 September 2024).

[5] See., e.g. review of the digitalization process in different policy sectors in: D. Gritsenko, M. Wijermars, M. Kopotev (Eds.). The Palgrave Handbook of Digital Russia Studies. Palgrave Macmillan, 2021.

provide a more stereoscopic view of the dynamics of this process, it is contextualized within the broader process of transformation of Russian society, with reference to official narratives of 'ontological security' and 'traditional values' that have significantly influenced regulatory policy in recent years.

The structure of the paper is based on the division of the issues that constitute the subject of the analysis into three specified clusters. Thus, Section One describes the key stages of the process of government digital transformation in Russia with the specific analysis of the "Electronic Russia" national program, its broad ambitions and unachieved goals. In Section Two, the turn to the technological independence and the 'sovereignization' of the national segment of the Internet is discussed, along with the concerns related the increasing degree of control over the information flows and extensive traffic filtering. Section Three is devoted to the discussion of the current stage of the digital transformation, both with its challenges to cybersecurity and aspirations for the leadership in the AI development. Section Four concludes the discussion.

It can be argued that the turn from a service model to ensuring technological sovereignty is underlying the current stage of digital transformation in Russia. The study of this phenomenon is more than timely and relevant against the backdrop of the growing isolation of the Russian segment of the Internet[6] and increasing political control by the state over online activity.

1. The e-government development in Russia: from the "Electronic Russia (2002–2010)" program to the present day

1.1. Theoretical framework for goal-setting of the e-government formation process

Though being a buzzword, 'e-government' lacks a widely accepted established definition. Layne and Lee define e-government as "government's use of technology, particularly web-based Internet applications to enhance the access to and delivery of government information and service to

[6] As the most prominent examples of Russian users being restricted from accessing foreign social networks and online platforms, in 2016 the social network LinkedIn was blocked by the Tagansky District Court of Moscow based on an appeal by *Roskomnadzor* due to violation of personal data legislation. In March 2022, *Roskomnadzor* blocked Facebook and then Twitter based on the request of the Prosecutor General's Office of 24 February in connection with the alleged dissemination of false information and calls to extremism against the background of the escalation of the armed conflict on the territory of Ukraine. Also in March 2022, the Tverskoy District Court of Moscow recognised the US company Meta, which operates the social networks Facebook and Instagram, as an extremist organization and banned its activities in Russia. Since the beginning of August 2024, Russian users see a slowdown of the popular video hosting site YouTube without an official announcement of its blocking. Against the backdrop of this slowdown, the media also reported that *Roskomnadzor* may spend almost 60 billion rubles (approximately $660 million) to update the system of blocking Internet resources in Runet, i.e. to fight VPN services (see: A. Gavrilyuk, RKN weaves new networks: the service will update the system of blocking websites for 59 billion rubles' [*RKN pletet novye seti: sluzhba obnovit sistemu blokirovki sajtov za 59 mlrd rublej*] (in Russian), Forbes (9 September 2024). https://www.forbes.ru/tekhnologii/520876-rkn-pletet-novye-seti-sluzba-obnovit-sistemu-blokirovki-sajtov-za-59-mlrd-rublej (accessed 11 September 2024).

citizens, business partners, employees, other agencies, and government entities".[7] Schelin describes the process of government digitalization as "revolutionizing the business of government through the use of information technology, particularly Web-based technologies, that improve internal and external processes, efficiencies, and service deliveries".[8] For the purposes of further discussion, a broad understanding of e-government is employed as the use of information and communication technologies, in particular the Internet, for execution of governmental functions.

Theories of the government digitalization discussed in scholarly literature[9] attempt to explain the complex dynamics of how technology shapes and is shaped by political processes, and in more practical terms — the reasons for governments to adopt digital technologies, the consequences of this adoption, and the ways in which technology can be used to achieve different political goals. David Garson developed four theories, or four approaches, for examining the e-government development.[10] Among them, the theory of *technological determinism* posits that technology is a driving force that shapes institutions and behaviors and pushes societies, including governments, to adapt.[11] Thus, technological determinists might argue that the Internet inevitably leads to increased transparency and citizen participation.[12] Though this theory offers a valuable framework for understanding the government digitalization, it faces criticism as oversimplifying the role of technology and overlooking the agency of individuals and institutions.[13]

---

[7] K. Layne, J. Lee, Developing Fully Functional e-Government: A Four Stage Model, Government Information Quarterly 18(2) (2001) 122–136, p. 123.

[8] S. H. Schelin, E-Government: An Overview, in: G. David Garson, Modern Public Information Technology Systems: Issues and Challenges, IGI Publishing, 2007, p. 113.

[9] See, e,g,: S. H. Schelin, Op.cit., p. 116-119; D. j. Calista, J. Melitski, E-government and E-governance: Converging Constructs of Public Sector Information and Communications Technologies, Public Administration Quarterly, 31(1/2) (2007) 87–120. JSTOR, http://www.jstor.org/stable/41288283; V. Homburg, Understanding E-Government: Information Systems in Public Administration (1st ed.). Routledge, 2008; J. Nograšek, M. Vintar, E-government and organisational transformation of government: Black box revisited?, Government Information Quarterly, 31(1) (2014) 108-118, doi.org/10.1016/j.giq.2013.07.006; M. Ayyad, How Does e-Government Work? In: Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance (ICEGOV '17). Association for Computing Machinery, New York, NY, USA, 2017, p. 485–493. doi.org/10.1145/3047273.3047310.

[10] G. D. Garson, Public Information Technology and e-Governance: Managing the Virtual State, Jones & Bartlett Learning, 2006.

[11] See also: G. Puron-Cid, J. Ramon Gil-Garcia, Performance and Accountability in E-Budgeting Projects, in: G. D. Garson, M. Khosrow-Pour (Eds.), Handbook of Research on Public Information Technology. Volume I / Information Science Reference, 2008, p. 722. For a general discussion on technological determinism refer, e.g., to: A. Dafoe, On Technological Determinism: A Typology, Scope Conditions, and a Mechanism. Science, Technology & Human Values 40 (2015). doi.10.1177/0162243915579283.

[12] M. Milakovich, The Internet and Increased Citizen Participation in Government, eJournal of eDemocracy & Open Government 2 (2010). doi.10.29379/jedem.v2i1.22; A. Fung, H. R. Gilman, J. Shkabatur, Six Models for the internet + politics, International Studies Review 15(1) (2013) 30–47. doi.org/10.1111/misr.12028; F. Tejedo-Romero, J. F. Ferraz Esteves Araujo, Á. Tejada, Y. Ramírez, E-government mechanisms to enhance the participation of citizens and society: Exploratory analysis through the dimension of municipalities, Technology in Society 70 (2022). doi.org/10.1016/j.techsoc.2022.101978.

[13] See, e.g.: D. MacKenzie, J. Wajcman, Introductory essay: the social shaping of technology, LSE Research Online. https://eprints.lse.ac.uk/28638/ (accessed 31 August 2024), p. 3.

The *reinforcement theory* argues that technology often serves to maintain the existing power structures and social inequalities.[14] It presupposes that technology is often used as a tool by those in power to maintain control and further their own interests. For instance, this theory might suggest that e-government platforms can be used to strengthen centralized control and limit dissent.[15] According to the *systems theory*, although technology does not automatically drive change, it has power to enable and facilitate the change, in particular, improve the efficiency and boost the performance of social institutions.[16] Advocates of this theory might point to how e-government systems can streamline administrative processes and improve service delivery.[17]

In contrast to the technology-centricity of the theories described, the *sociotechnical theory* brings in a broader socio-political context and emphasizes the role of human agency in shaping the outcomes of technological change.[18] It recognizes that technology is implemented alongside individual practices, perceptions and choices, influencing how technology is developed and used.[19] In terms of this theory, e-government platforms can be designed to support decentralization and citizen participation, or conversely, to strengthen centralized control, depending on the choices made by policymakers and developers.

Apart from the four theories developed by Garson, the *legitimation theory*, developed particularly by the authors exploring the digital transformation in hybrid and authoritarian regimes, argues that digitalization can be used as a tool for enhancing legitimacy: namely, e-government platforms can create an illusion of transparency, participation and efficiency, helping governments maintain their grip on power while seemingly embracing modern technology.[20]

These theories are not mutually exclusive. As will be shown further on the example of the stages of the government digital transformation in Russia, the adoption and use of digital

[14] J. Melitski, D. Calista, E-Government and E-Governance Best Practices in Cities and Countries Compared between 2003 and 2012: Fad or Diffused Innovation? Public Administration Quarterly 40(4) (2016) 913-948. https://doi.org/10.1177/073491491604000408.
[15] T. Dragu, Y. Lupu. Digital Authoritarianism and the Future of Human Rights, International Organization 75(4) (2021) 991–1017. https://doi.org/10.1017/S0020818320000624.
[16] E. F. Rafael, Technology as a Social System: A Systems Theoretical Conceptualization, Philippine Sociological Review 61(2) (2013) 319–47.
[17] D. West, E-Government and the Transformation of Service Delivery and Citizen Attitudes, Public Administration Review. 64 (2004) 15-27. doi:10.1111/j.1540-6210.2004.00343.x.
[18] N. Fair, Industry5.0 and Sociotechnical Theory: Theoretical Underpinnings, Proceedings of the Workshop of I-ESA'22, (2022), Valencia, Spain. https://ceur-ws.org/Vol-3214/WS5Paper4.pdf (accessed 31 August 2024).
[19] L. Kompella, Socio-Technical Transitions and Organizational Responses: Insights from E-Governance Case Studies, Journal of Global Information Technology Management 23(2) (2020) 89–111. doi:10.1080/1097198X.2020.1752082.
[20] S.C. Greitens, Authoritarianism Online: What Can We Learn from Internet Data in Non-democracies?, PS: Political Science & Politics 46(2) (2013) 262–270; S.F. Maerz, The Electronic Face of Authoritarianism: E-Government as a Tool for Gaining Legitimacy in Competitive and Non-competitive Regimes, Government Information Quarterly 33(4) (2016) 727–735.

technologies in government are influenced by a combination of factors, including technological advancements, social and political structures, and the motivation for uptake of information technologies by the government, which can change over time. A comprehensive understanding of the government digitalization requires examining these factors in their interplay.

1.2. Starting point of the digitalization of public administration: the "Electronic Russia (2002–2010)" program

The task for digitalizing the process of providing public services and forming e-government was outlined in the early 2000s by the Federal Target Program "Electronic Russia (2002–2010)".[21] The key objectives of the program were to create conditions for the development of democracy, increase efficiency in the functioning of the economy and national and local governance, ensure the rights to free search, access, transmission, production and dissemination of information, and build the information and communication technologies (the 'ICTs') capacity.[22] In retrospect, it now appears that the goals stated in the program, in particular to ensure greater openness of the government institutions to citizens, were not nominal or declarative: by the early 2000s there was still a clear demand in the Russian society for freedom, the rule of law and effective institutions of democracy — the values that Russian citizens had enthusiastically embraced during the years of *perestroika* and the first decade of the post-Soviet period.[23] Thus, the availability of information to the citizens and their free access to information on the activities of government bodies, at least at the federal level, were the cornerstones of the early e-government process.[24]

Herewith, the first years of the implementation of the "Electronic Russia" program highlighted the problem of the lack of necessary equipment and the construction of infrastructure that would ensure the automation of basic processes in public administration, even at the level of individual departments of governmental authorities.[25] The key targets of the government capital investments in 2005–2006 were the acquisition of equipment and the creation of necessary software and hardware systems, which, however, were accompanied by accusations and

[21] Federal Target Program "Electronic Russia (2002–2010)", approved by Resolution of the Government of the Russian Federation of 28 January 2002 No. 65. https://digital.gov.ru/ru/activity/programs/6/ (accessed 10 September 2024).
[22] ibid.
[23] See, e.g.: O. Malinova, Encounters with liberalism in Post-Soviet Russia, in: M. Freeden, J. Fernández-Sebastián, J. Leonhard (Eds.), In Search of European Liberalisms: Concepts, Languages, Ideologies, New York, Oxford: Berghahn Books, 2019. P. 278-301.
[24] D. J. Peterson, Russia and the Information Revolution. Santa Monica, CA: RAND Corporation, 2005. P. 58.
[25] D. Gritsenko, M. Zherebtsov, E-Government in Russia: Plans, Reality, and Future Outlook, in: D. Gritsenko, M. Wijermars, M. Kopotev (Eds.). The Palgrave Handbook of Digital Russia Studies. Palgrave Macmillan, 2021, p. 38.

investigations into the misuse of budgetary funds.[26] The lack of effectiveness in the program implementation was recognised by officials even before its completion.[27] A post facto expert review showed that many of the key objectives of the program remained unresolved, including preferential use in public services of algorithms and programmes, the texts of which are open and publicly available; the ICTs-based implementation of procedures for interaction between the federal agencies and business entities in the area of accounting, registration, licensing and state reporting; and the implementation of electronic document management in public authorities using electronic digital signature.[28]

Despite these shortcomings in the implementation of the "Electronic Russia" program, its main result was the launch on 15 December 2009 in test mode, and from 1 January 2010 – full-scale, of the Unified Portal of State and Municipal Services, known as *Gosuslugi* (the 'Government Services') and now managed by *Rostelecom*, the largest shareholder of which is the Russian Federation, represented by *Rosimushchestvo* (the Federal Agency for State Property Management). After over a decade of rapid development, *Gosuslugi* has become a universal means of obtaining federal and municipal services of all sorts, including, making an appointment with a doctor, submitting applications to the registry office, issuing a foreign or national passport, a driver's license and other documents, paying state fees, taxes and fines (with a discount of up to 50%), registration of rights to real estate — more than 970 services in total.[29] The number of verified users in 2023 exceeded 103 million.[30] The portal can also be used by foreign citizens, in particular citizens of CIS countries and others permanently or temporarily residing and working in Russia.

The increase in the openness and accessibility of information on the activities of state bodies, as well as simplified electronic interaction with citizens during this period, was also

[26] I. Tsukanov, N. Biyanova, A. Nikolsky, One-sixth of the budget of the Electronic Russia programme stolen [*Ukradena shestaja chast' bjudzheta programmy «Jelektronnaja Rossija»*] (in Russian), Vedomosti (31 August 2011). https://www.vedomosti.ru/politics/articles/2011/08/31/hischenie_po_programme (accessed 11 September 2024).

[27] 'Sergey Ivanov is dissatisfied with the current results of the implementation of the Federal Target Programme 'Electronic Russia' [*Sergej Ivanov nedovolen tekushhimi rezul'tatami vypolnenija FCP "Jelektronnaja Rossija"*] (in Russian), Cnews (19 March 2007). https://www.cnews.ru/news/line/sergej_ivanov_nedovolen_tekushchimi_rezultatami_1 (accessed 11 September 2024).

[28] Higher School of Economics, with the participation of the World Bank, Digital Transformation State Government: Myths and Reality [*Cifrovaja transformacija gosudarstvennogo upravlenija: mify i real'nost'*] (in Russian), Publishing House of the Higher School of Economics, 2019. https://publications.hse.ru/books/263485886 (accessed 11 September 2024). P. 11.

[29] What is *Gosuslugi* [*Chto takoe Gosuslugi*] (in Russian). https://www.gosuslugi.ru/help/faq/general/2373 (accessed 11 September 2024).

[30] 'Chernyshenko: the Number of Verified Users of *Gosuslugi* has Reached 103 Million' [*Chernyshenko: chislo verificirovannyh pol'zovatelej Gosuslug dostiglo 103 mln*] (in Russian), Interfax-Russia (14 August 2023). https://www.interfax-russia.ru/main/chernyshenko-chislo-verificirovannyh-polzovateley-gosuslug-dostiglo-103-mln (accessed 11 September 2024).

reflected in launching of several key federal information portals, such as *Goszakupki* (the 'Government procurement'), state automated system *Vybory* (the 'Elections'), *Pravosudie* (the 'Justice') and the platform for public discussion of draft laws — the Federal Portal of Draft Normative Legal Acts, better known by the name of its Internet page address as '*Regulation.gov.ru*'.[31] Overall, the government openness indicators have improved significantly: the Government Transparency Index, which measures the availability of credible aggregate economic data that a state discloses to the public, was negative in Russia in 1990 (-0.98), below most Western European countries in 2000 (4.72 in Russia, in comparison with, for example, 5.15 in France, 6.53 in Finland, 7.26 in Sweden, 7.78 in Spain) and at the European level in 2005 (6.22 in Russia, 6.78 in France, 6.50 in Finland, 6.20 in Sweden, 7.08 in Spain).[32]

1.3. The conservative turn in domestic politics after the Crimean crisis and the course towards technological independence

After the end of the federal program "Electronic Russia", and against the background of the reform of the public administration system, the e-government initiative has received a second wind through the initiative on creation of the so called 'information society'. In 2017, the "Strategy for the Development of the Information Society in the Russian Federation for 2017–2030" was approved by the Decree of the President.[33] The purpose of this Strategy is defined as creation of conditions for the formation of the knowledge society in Russia. Thus, the document is full with declarations of a humanitarian nature on the government's efforts towards implementing educational projects, creating a publicly accessible system of interconnected knowledge and ideas for citizens, ensuring a safe information environment for children, promoting the Russian language in the world, supporting traditional forms of knowledge dissemination (other than through the Internet).[34] However, most of these provisions are not accompanied by mechanisms for effective implementation and monitoring.

What is important in the context of this discussion is not the declarative provisions of the Strategy on the formation of a knowledge society, but the course it takes to ensure Russia's technological independence (primarily from Western technologies and software). Thus, the

[31] More on digitalization of the legal process in Russia, see e.g. M. Muravyeva, A. Gurkov, Law and Digitization in Russia, in: D. Gritsenko, M. Wijermars, M. Kopotev (Eds.). The Palgrave Handbook of Digital Russia Studies. Palgrave Macmillan, 2021.
[32] Human Progress, Government Transparency Index. https://humanprogress.org/dataset/government-transparency-index/ (accessed 11 September 2024).
[33] Decree of the President of the Russian Federation dated 9 May 2017 No. 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 – 2030".
[34] ibid, Art 25.

Strategy lists the following areas of development among priorities: creation and application of Russian ICTs, ensuring their competitiveness at the international level, and securing national interests in the field of digital economy.[35] The latter includes, in particular, ensuring technological independence and security of the infrastructure used to sell goods and provide services to Russian citizens and organizations.[36] Thus, the development of national IT solutions and infrastructure were prioritized. As will be shown below, similar statements about the need to ensure technological independence are becoming typical for documents in the field of digitalization in recent years.[37] Overall, this period marks the change of rhetoric and goal-setting from modernization to ensuring national security and, what has become a cliché in bureaucratic parlance, 'technological sovereignty' alongside the 'economic sovereignty'.[38] It seems that this turn can be seen as one of the manifestations of a more general trend towards conservatism in national politics during this period, and a certain disappointment in the upper echelons of power about the possibilities of cooperation with foreign partners (if not outright confrontation with Western states) in the circumstances of sanctions pressure since 2014 following the events in Crimea and, in this connection, efforts to reduce the technological lag and ensure the possibility of functioning independently of foreign technologies.

During the same period, the widely acclaimed 'Yarovaya Law'[39] was passed, which introduced amendments to the legislation on combating terrorism and ensuring public security. The law introduced requirements for the localization of users' data: namely, it required telecom companies, messengers, e-mail services and other distributors of information on the Internet to store on the territory of Russia (i) information on the facts of reception, transmission, delivery and/or processing of voice information, written text, images, sounds, video or other electronic messages of users and information about such users; and (ii) users' text messages, voice information, images, sounds, videos and other electronic messages. Data storage periods range from six months to three years, during which time the operator is required to make user data

[35] ibid, Art 22.
[36] ibid, Art 42(e).
[37] See, e.g., the "Strategy for the Scientific and Technological Development of the Russian Federation" approved by the Decree of the President of the Russian Federation dated 1 December 2016 No. 642, Art 28: "The goal of scientific and technological development of the Russian Federation is to ensure the independence and competitiveness of the country through the creation of an effective system for building up and making the fullest use of the intellectual potential of the nation".
[38] A. A. Egorova, I. A. Danilov, I. P. Dovbiy, Evolution of the concept and characteristics of technological sovereignty: a retrospective analysis and prospects in conditions of increased volatility of the economy, Bulletin of Chelyabinsk State University. 12(470) (2022) 33-44. (In Russian)
[39] Federal Law dated 6 July 2016 No. 374-FZ "On the Adoption of Amendments to the Federal Law 'On Countering Terrorism' and Specific Legislative Acts of the Russian Federation Regarding the Establishment of Additional Counter-terrorism Measures and Ensuring Public Security'.

available to law enforcement agencies upon their request. The Yarovaya Law has been widely criticized not only for potentially violating the constitutional rights of citizens to privacy[40] and creating an accumulation of data that is attractive to cyberattacks,[41] but also for being disastrous for the industry — forcing operators and Internet companies to increase the capacity of their data centres and raising the cost of services to end users due to operators' additional expenses.[42]

The trend towards greater independence from foreign technologies continues in the current stage of digitalisation of the public administration system. Thus, in November 2023 the Russian Government decided that in the period from 1 September 2024 to 1 January 2030, all operators of the critical information infrastructure are required to switch over to Russian software and equipment: the current foreign-made equipment will be gradually replaced by equipment and software that is listed in the Russian radio-electronic products and software registers.[43]

1.4. Digitalization challenges amid the COVID-19 pandemic and the partial mobilization

The process of government digital transformation continues, although it is currently complicated by additional challenges, both of purely technological nature (such as increasing role of the AI technology) and organizational nature (for instance, the departure of a significant number of highly qualified IT specialists from Russia following the announcement of partial mobilization in September 2022, some of whom continue to work remotely for Russian companies[44]). In 2019, a key federal program in the field of the public services digitalization was adopted — the "Digital Economy of the Russian Federation"[45] — with a planned annual budget of US$1.8 billion until

[40] E. Moyakine, A. Tabachnik, Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology, Computer Law & Security Review 40 (2021) paper 105512. doi.org/10.1016/j.clsr.2020.105512.

[41] E. Vinogradova, P. Kantyshev, E. Sergina, Who Can Make Money on the Yarovaya Law [*Kto mozhet zarabotat' na zakone Jarovoj*] (in Russian), Vedomosti (21 August 2016). https://www.vedomosti.ru/technology/articles/2016/08/22/653895-kto-zarabotaet-zakone-yarovoi (accessed 21 October 2024).

[42] According to the conclusion of the Commission of the Russian Union of Industrialists and Entrepreneurs on Communications and Information and Communication Technologies. See: Human Rights Council under the President of the Russian Federation, Media: Telecom operators will have to spend RUB 10 trillion on the Yarovaya Law [*SMI: Operatoram svjazi pridetsja potratit' 10 trln rublej na "zakon Jarovoj'*] (in Russian). https://www.president-sovet.ru/presscenter/press/smi_operatoram_svyazi_pridetsya_potratit_10_trln_rubley_na_zakon_yarovoy/ (accessed 21 October 2024).

[43] Resolution of the Government of the Russian Federation dated 14.11.2023 No. 1912 "On the Procedure for the Transition of Subjects of Critical Information Infrastructure of the Russian Federation to the Primary Use of Trusted Software and Hardware Systems at Significant Objects of Critical Information Infrastructure of the Russian Federation belonging to them".

[44] A. Zlobin, The head of the Ministry of Digitisation says 100,000 IT specialists have left Russia [*Glava Mincifry soobshhil o 100 000 uehavshih iz Rossii ajtishnikov*] (in Russian), Forbes (20 December 2022). https://www.forbes.ru/tekhnologii/482755-glava-mincifry-soobsil-o-100-000-uehavsih-iz-rossii-ajtisnikov (accessed 14 September 2024).

[45] Approved by the minutes of the meeting of the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects dated 4 June 2019 No. 7.

2025. The program aims at design of normative regulation of the digital environment, support for the human resources in the IT industry and education, maintenance of information infrastructure and information security, digital public administration, development of the AI and expanding Internet coverage through the development of satellite communications.[46] Within the framework of the federal project, the conditions for the collection, storage and processing of data using new technologies have been created, among other things; the specifics of the processing of personal data authorized by the data subject for dissemination have been outlined, which will increase the control of the data subject over the processing of her personal data authorized for dissemination.[47]

Like in many other states, the COVID-19 pandemic has become a stress test for the Russian Internet-based state services provision system. One of the consequences that the pandemic had on the digitalization process in Russia was the expansion of the functionality of the *Gosuslugi* portal — registration for vaccination and issuance of COVID-19 vaccination certificates were also implemented there. The pandemic also gave impetus to the development of telemedicine solutions. The development of telemedicine platforms was one of the factors that allowed Moscow to enter the top three (after San Francisco and New York) in the ranking of combatting COVID-19 innovations.[48] Telemedicine centers were established in all Russian regions; federal telemedicine centers also provided teleconsultations on the treatment of COVID-19 to regional hospitals. Despite the fact that telemedicine technology increases the accessibility of medical care, its use in the public healthcare system is also associated with inequalities. Certain ethnic, socioeconomic groups and minorities, such as patients with speech disorders, deaf people, elderly patients and disabled people with a low level of digital competence, residents of rural and remote areas without full Internet access, were less able to access remote health services during the pandemic.[49] The telemedicine technologies, being actively implemented in the public healthcare system during post-COVID-19 era, should not create additional barriers to the access to professional medical care. Ensuring the inclusivity of telehealth platforms is possible through technical solutions proposed by Russian researchers, in particular, through the use the ISA 315 Organization's Internal Control System with its D&I component.[50]

---

[46] Description and metrics of all the directions are available on the official Internet page of the program (in Russian). https://digital.gov.ru/ru/activity/directions/858 (accessed 14 September 2024).
[47] Federal Law dated 30 December 2020 No. 519-FZ "On Amendments to the Federal Law 'On Personal Data".
[48] StartupBlink, Global Rankings of Cities on Coronavirus Resilience Innovation. https://coronavirus.startupblink.com/ (accessed 14 September 2024).
[49] M. Dvoryashina, E. Tarasenko, Inclusion, Diversity Or Disparity In Telehealth During The Covid-19 Pandemic, IFAC-PapersOnLine 54(13) (2021). https://www.sciencedirect.com/science/article/pii/S2405896321019042 (accessed 14 September 2024). P. 323, 324.
[50] ibid, p. 326.

Next, the beginning of the special military operation in Ukraine and subsequent partial mobilization caused the transition of the conscription process to electronic form and creation of a special register of military enlisting (the 'Register')[51] integrating information from other existing registries and databases: those operated by the Ministry of Internal Affairs, the Federal Tax Service, the Central Election Commission, the Pension Fund of Russia (now Social Fund of Russia), the Ministry of Education, the Ministry of Healthcare and other departments. The Register is filled with data from the state bodies' databases by means of interdepartmental electronic interaction, as well as by submission of the information from employers, without the participation of citizens. At the same time, electronic military summonses (*povestki*) were introduced. Previously, there was only one legal way to serve a summons – personally in hand with written acknowledgement of receipt. From now on, summons will be sent both in hard copy and electronically, that is by means of deposition in the personal account on *Gosuslugi* portal. In addition, summons will be placed on the Register and considered delivered after seven days from the date of being uploaded to the Register. Immediately upon sending an electronic summons, the individual is automatically restricted from leaving the country until he appears at the military registration office. In case of non-attendance within 20 days, additional restrictions apply which include a prohibition on state registration as an individual entrepreneur or self-employed (popular tax regimes for self-employment and freelancing); a prohibition of state registration of rights to real estate (which makes it impossible to sell, gift or otherwise dispose of one's real estate); a prohibition of state registration of vehicles and a restriction on their use (a driving license is blocked); and a ban on receipt of a bank loan. Adoption of the described amendments to the legislation on military duty raises serious concerns about respect for the rights and legitimate interests of conscripts during the process of conscription. Moreover, the traditional formula for understanding citizenship as a stable legal relationship between a person and the state is increasingly drifting towards the legal relationship between the 'digital image' of a person and the state, as the civil rights of a significant part of Russian citizens are being made dependent on an electronic entry related to their attitude towards military duty.

[51] Federal Law dated 14 April 2023 No. 127-FZ "On Amendments to Certain Legislative Acts of the Russian Federation" introducing amendments to the Federal Law dated 28 March 198 No. 53-FZ "On Military Duty and Military Service".

1.5. Looking forward: strategic planning for the development of the communications industry till 2035

In August 2023, the "Strategy for the Development of the Communications Industry of the Russian Federation for the Period until 2035" (the 'Communications Industry Strategy')[52] was presented by the Ministry of Digital Development, Communications and Mass Media for the public consultation.[53] The Communications Industry Strategy highlights the challenges faced by the industry because of current sanctions restrictions on the supply of equipment and software. The need to ensure technological sovereignty in the communications industry is emphasized, and the 'technological sovereignty' is described as the state's ability to ensure controllability of telecommunication networks and all user devices (including any devices that generate an electrical signal and transmit information) located within the Russian territory.[54] Ensuring technological sovereignty is expected in two main forms: research, development and implementation of critical and end-to-end technologies; and manufacturing of high-tech products based on these technologies.[55] The Communications Industry Strategy also calls for a revision of approaches to the use of the foreign-made telecommunications equipment and introduction into the Russian legislation of the category 'trusted telecommunications equipment' — that is, the equipment which meets the information security requirements to be established by authorized bodies, followed by a transition to using predominantly 'trusted equipment' to perform certain functions in communication networks.

The current stage of the process of public administration digitalization is characterized by a number of problems, including, a large number of regulatory legal acts, their unsystematic and multidirectional, point-by-point changes; growth of control and supervisory functions of industry regulators; imposing additional responsibilities on telecom operators related to the regulation of related industries. Currently, legislation in the field of IT and communications is distributed between numerous legislative acts (at least 60 according to the most conservative estimates[56]). To address this problem, the Communications Industry Strategy proposes to develop the Digital Code — a legislative act that systemises industry legal norms and provides comprehensive regulation of

[52] The text of the Communications Industry Strategy and explanatory note to it are available on the official Internet page of the strategy (in Russian). https://digital.gov.ru/ru/documents/9120/ (accessed 14 September 2024).
[53] The results of the public consultation are available on the Internet page of the State automated information system "*Upravlenie*" ('Management') (in Russian). https://gasu.gov.ru/stratpassport (accessed 14 September 2024).
[54] Communications Industry Strategy, Sec 2.10.
[55] ibid.
[56] The central pieces of legislation in the field include: the Federal Law dated 27 July 2006 No. 149-FZ "On Information, Information Technologies and Information Protection", the Federal Law dated 7 July 2003 No. 126-FZ "On Communications", the Federal Law dated 27 July 2006 No. 152-FZ "On Personal Data".

the development and use of information technologies and communication infrastructure both in the public and private sectors.[57] It is expected that the Digital Code will consolidate and systematize legislation in the industry: it will include, inter alia, provisions on the protection of personal data and digital identification of citizens, develop a legal framework for the use of Big Data, introduce the regulation of cloud technologies and non-state services, as well as liability mechanisms when using AI, including for resolving judicial issues.[58] Herewith, the feasibility of the ambitious goal of developing a comprehensive act in the form of a Digital Code by 2025 is questionable. In the Russian legal system, codification is the highest form of systematization of legal norms within a branch of law. During codification, not only normative material is collected, but also gaps and contradictions are eliminated, a general conceptual apparatus is developed. One of the characteristics of legal regulation by a codified act is stability — any code is intended to regulate the most important areas of public relations during a prolonged period of time. Despite the fact that the Russian legal system has accumulated a large number of IT-related norms, it seems that they are not ready for codification due to the lack of theoretically developed concepts and approaches to defining key categories (and without this, the mechanical combination of several laws will give birth to a kind of legal Frankenstein), as well as due to the dynamic nature of the industry development requiring active changes in legislation following the development of technology, which is not quite typical for such an act as a code. In general, the idea of creating a Digital Code today seems to be more an element of international competition and a desire to show progressiveness than a real need for the legislative system.

2. Efforts towards 'sovereignization' of the national segment of the Internet

As a next step, beyond the task of technological independence, a set of regulations was adopted to ensure the potential autonomy of the Russian segment of the Internet. In November 2019, the so-called 'Sovereign RuNet Law' came into force.[59] The explanatory note to the law stated that its goal is to ensure the functionality of the Internet in Russia in the event of its disconnection from the global network. New responsibilities were assigned to telecom operators, and a duty to monitor that databases and programs associated with public service provision are located in Russia was imposed on the government agencies. The telecom regulator — *Roskomnadzor* (Federal Service

[57] Communications Industry Strategy, Sec IV.
[58] T. Isakova, They Write a Code for IT [*Dlja IT pishut kodeks*] (in Russian), Kommersant (8 November 2023). https://www.kommersant.ru/doc/6321957# (accessed 14 September 2024).
[59] Federal Law dated 1 May 2019 No. 90-FZ "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection".

for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications) — received additional powers to block traffic on the Internet.

Under the Sovereign RuNet Law telecom operators are required to install special equipment (in the terminology of the law, 'technical means of countering threats') to prevent a potential shutdown of the Internet in Russia.[60] In the event of threats to the stability, security and integrity of the functioning of the Internet on the Russian territory, *Roskomnadzor* can exercise the so-called 'centralized management' of the public communications network.[61] The threats to security which trigger the exercise of such management include, inter alia, attempts of an unauthorized access to hardware and software of a public communications network, deliberate destabilization of internal or external information impacting attacks that disrupt the functioning of a public communications network, along with attacks associated with the dissemination of information on the Internet, access to which is restricted under the Russian legislation.[62]

In fact, this is a very wide range of cases that give grounds for *Roskomnadzor* to undertake measures up to and including blocking the Internet traffic without the participation of telecom operators.[63] Thus, in accordance with the Rules for Centralized Management of a Public Communications Network, introduced by the Government, on 1 March 2022 *Roskomnadzor* started restricting access to the Twitter social network by 'slowing down' access to the social network traffic based on the accusations of disseminating "unreliable socially significant information" about the Russia's military operation in Ukraine.[64] Later, the access to the social network on the territory of Russia was limited on the basis of Article 15.3 of the Federal Law "On Information, Information Technologies and Information Protection", which regulates the procedure for limiting access to the Internet resources containing calls for mass riots, extremist activities, participation in mass (public) events held in violation of the established procedure.[65]

Such a practice of the expanding filtering and blocking of the Internet content by a regulator reflects the trend of a greater state involvement in the Internet governance, which is currently

[60] Art 46(5.1.) of the Federal Law "On Communications" as amended by the Federal Law dated 1 May 2019 No. 90-FZ.
[61] Ibid, Art 65.1(2).
[62] Resolution of the Government of the Russian Federation dated 12 February 2020 No. 127 "On Approval of the Rules for Centralized Management of a Public Communications Network", Art 5.
[63] I. Stadnik, Sovereign RUnet: What Does it Mean?, Internet Governance Project. Georgia Institute of Technology. 12 February 2019. https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/ (accessed 12 September 2024).
[64] R. Tairov, In Russia, Following Facebook, Twitter was Blocked [*V Rossii vsled za Facebook zablokirovali Twitter*] (in Russian), Forbes (4 March 2022). https://www.forbes.ru/tekhnologii/458149-v-rossii-vsled-za-facebook-zablokirovali-twitter (accessed 11 September 2024).
[65] Russia Restricts Access to Twitter [*V Rossii ogranichili dostup k Twitter*] (in Russian), TASS (4 March 2022). https://tass.ru/obschestvo/13969933 (accessed 11 September 2024).

observed in different states, irrespective of whether they are democratic or not.[66] In Russia, this trend involves also the efforts to isolate the national physical infrastructure from the global network. Thus, on 1 January 2018, the Federal Law No. 187-FZ "On the Security of Critical Information Infrastructure" came into force (the 'CII Law'). The CII Law is intended to ensure the security of information infrastructure facilities of the Russian Federation, the functioning of which the state considers critically important. The CII Law defines the significant critical information infrastructure (the 'CII') object enumerating the areas in which relevant information systems and networks operate: healthcare, science, transport, communication, power engineering, banking and other areas of the financial market, fuel and energy complex, atomic energy, defence and rocket and space industry, mining, metallurgical and chemical industries.[67] Thus, physical objects of information infrastructure and telecommunication networks used to organize interaction between them constitute the concept of CII. Operators of the significant CII object are required to immediately inform the federal executive body of cyber incidents against the CII objects. Moreover, this executive body is entitled to conduct regular and unscheduled on-site inspections of the CII facilities operators to monitor their compliance with the requirements of the CII Law.[68]

As part of the efforts to ensure stability of the Russian segment of the Internet in the event of disconnection it from the global network, the national domain name system (the 'DNS') was introduced in 2021. The Center for monitoring and control of the public telecommunications network released the instruction of four pages for connecting telecom operators and owners of autonomous systems to the national DNS.[69] It contains configuration examples for several of the most popular DNS servers. The owners of the autonomous system numbering resource are expected to configure their DNS servers so that they receive the root zone of one of the addresses listed in the instruction or simply give their clients addresses that were issued. All requests to the national domain name system go through the Center which is subordinate to *Roskomnadzor*. The main task of the Center is to monitor situation and, in case of emergency, to coordinate actions of telecom operators. The latter, in turn, are obliged to provide complete information about their

[66] I. Stadnik, Russia: An independent and sovereign internet?, in: B. Haggart, N. Tusikov, J. A. Scholte (Eds.), Power and Authority in Internet Governance: Return of the State?, Routledge, London, 2021. P. 147.
[67] The CII Law, Art 2(8).
[68] Resolution of the Government of the Russian Federation dated 17 February 2018 No. 162 "On Approval of the Rules for the Implementation of State Control in the Field of Ensuring the Security of Significant Objects of Critical Information Infrastructure of the Russian Federation".
[69] *Roskomnadzor*, 'Instructions for Connecting Telecom Operators and Owners of Autonomous Systems to the National Domain Name System (NSDN) approved by the Center for Monitoring and Control of the Public Communications Network. https://25.rkn.gov.ru/docs/25/sm33732/Instrukcija_dlja_OS_po_podkljucheniju_k_NSDI_v4.pdf (accessed 11 September 2024).

users, including SSL sessions, logins and IP addresses which gives cause for concern that *Roskomnadzor* will collect users' data including their web browsing history.

The developments of the national regulation towards greater control over the information infrastructure and DNS can be perceived as an element of the threefold framework of what Milton Mueller calls 'the alignment of cyberspace to national borders', consisting of securitization of cyberspace, territorialization of information flows and national regulation of the Internet names and numbers.[70] Herewith, such alignment of cyberspace specifically to the Russian national borders within the framework of legislation on the Sovereign RuNet and CII is questionable. These doubts are related both to purely technical issues (including, first and foremost, the still high degree of dependence of the Russian networks on external connections, compared particularly with China[71]) and the regulation deficiencies.[72] What is undeniable is the increasing degree of the control over the information flows and extensive traffic filtering.[73]

3. Current challenges of digital transformation: cybersecurity and AI regulation

3.1. Cybersecurity agenda and related data security issues

The issue of cybersecurity (or 'information security', as it is traditionally referred to in Russian official documents[74]) has become of fundamental importance to Russia in recent years for several reasons. First, against the backdrop of the military operation in Ukraine, the number of cyberattacks on Russia's cyber infrastructure has increased significantly. Thus, since October 2023, the Main Intelligence Directorate of the Ukrainian Ministry of Defense has openly acknowledged the authorship of at least five episodes of cyberattacks, the most plausible of which was the statement about an attack on the Russian company *IPL Consulting* which develops and

[70] M. Mueller, Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace, London: Polity, 2017.
[71] E. Zinovieva, B. Yajie, Digital Sovereignty in Russia and China, Russian International Affairs Council, 11 June 2023. https://russiancouncil.ru/en/analytics-and-comments/analytics/digital-sovereignty-in-russia-and-china/ (accessed 10 September 2024).
[72] As Ilona Stadnik so aptly put it, the analysis of the Sovereign RuNet Law "leaves the impression that it was written by people who see the internet as being similar to telephone communications". See: I. Stadnik, Russia: An independent and sovereign internet?, in: B. Haggart, N. Tusikov, J. A. Scholte (Eds.), Power and Authority in Internet Governance: Return of the State?, Routledge, London, 2021. P. 160.
[73] See, e.g.: A. A Efremov, Formation of the Concept of Information Sovereignty of the State, Pravo. Zhurnal Vysshey shkoly ekonomiki 1 (2017) 201–215 (in Russian). P. 203.
[74] In the Doctrine on Information Security of Russia (approved by the Decree of the President of the Russian Federation dated 5 December 2016 No. 646), the information security is defined as "station of security of an individual, the society and the state from internal and external information threats at which are provided: implementation of the constitutional rights and freedoms of an individual and the citizen; good quality of living for citizens; sovereignty, territorial integrity and sustainable social and economic development of the Russian Federation; defense and security of the state".

implements technological solutions for managing processes in heavy industry.[75] The statements of the Ukrainian agency, especially of 12 December 2023 on hacking of the Federal Tax Service of Russia[76] and of 17 August 2024 on attacking an Internet provider in Snezhinsk (Chelyabinsk region) resulting in the disconnection from the Internet of a number of strategic enterprises in the city, including VNIITF (a research institute within Rosatom's system that develops nuclear warheads),[77] are unprecedented — there have never been cases before when a state proactively acknowledged a destructive cyberattack on nuclear and civilian cyber infrastructure. Probably, official statements on behalf of a Ukrainian governmental agency are designed for mostly informational effect. Still, they show that many former taboos on consideration of the military use of cyber capabilities have been lifted and make the task of ensuring Russia's national security in cyberspace more urgent than ever before.

Second, Russia is not only a frequent victim state but is also constantly accused of sponsoring malicious cyber actions: 48 states are suspected of sponsoring cyber operations for the period from 2005 to 2023 inclusive, and in this list China, Russia, Iran, and North Korea are designated as responsible for up to 82% of all cyber operations of this type.[78] Therefore, the formation of a national position on so-called 'international information security' (the international legal dimension of cybersecurity, as it is known in Russian discourse) has traditionally been a priority. At the same time, Russia is looking for opportunities to cooperate with other 'like-minded' states on issues related to cybersecurity, both bilaterally and under the aegis of BRICS and, particularly, the Shanghai Cooperation Organisation (the 'SCO').[79] Cooperation within the SCO contemplates the establishment of a system for monitoring and joint response to threats arising in this area, countering threats of the use of ICTs for terrorist purposes, ensuring the information security of critical structures of the SCO member states, exchanging information on the legislation of SCO member states on ensuring information security, exchanging experience,

[75] M. Fornusek, Military Intelligence Claims Cyberattack on IT Company Providing Services to Russian Defense Industry, The Kyiv Independent (27 January 2024). https://kyivindependent.com/military-intelligence-claims-powerful-cyberattack-on-russian-it-company (accessed 13 September 2024).
[76] @ DIUkraine, 12 December 2023. https://t.me/DIUkraine/3194 (accessed 4 May 2024).
[77] @ DIUkraine, 17 August 2024. https://t.me/DIUkraine/4266 (accessed 19 August 2024).
[78] Council of Foreign Relations. www.cfr.org/cyber-operations/.
[79] See, e.g.: the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security signed 16 June 2009, entered into force on 5 January 2012. https://base.garant.ru/2571379 (accessed 13 September 2024); the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security dated 8 May 2015, entered into force on 10 August 2016. http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1 (accessed 13 September 2024); the XIV BRICS Summit Beijing Declaration, 23 June 2022. http://en.kremlin.ru/supplement/5819 (accessed 13 September 2024).

training specialists, holding working meetings, seminars and conferences, as well as the exchange of data on information security issues.[80] Despite the positive dynamics in the joining of efforts in the field of international information security in Eurasia, it is necessary to point out the existing problems and obstacles to the effective cooperation in the region. The main difficulties include a relatively low level of trust and a high level of competition for leadership in cyberspace (primarily between China and Russia). As ICTs today play a critical role for both military and civilian sectors, the 'stakes' for overall national security are high, and states tend to be driven primarily by national interests rather than seeking comprehensive cooperation.

Finally, attacks on government agencies not only damage the information infrastructure, but also threaten data security. According to Positive Technologies, one of the leaders in the Russian cybersecurity market, government agencies worldwide, and in Russia in particular, in the three quarters of 2023 remained the main targets of malicious cyberattacks.[81] The consequence of attacks is both an intervention in the core activity of the agency and, in 42% of cases globally, a leak of confidential information.[82] The Russian public sector is especially vulnerable in the current geopolitical situation, and for 2025 an increase in the number of incidents is expected with potentially devastating consequences, which could also affect critical government services and cause leaks of both personal data and confidential government information. Accordingly, the legislator is concerned with protection of the personal data and liability for violations of the data processing procedures. In January 2024, the State Duma – the lower house of the Russian parliament adopted in the first reading two bills: the first one introduces turnover fines (depending on the number of affected personal data subjects) of up to 500 million rubles (approx. $5.5 million) for companies and individuals responsible for data leakage;[83] the second bill introduces criminal liability for the illegal collection, storage, use and (or) transfer of computer information with personal data.[84] The purpose of the bills, as stated by the initiators, is to protect data from leakages, including deliberate ones by employees of companies – data operators for personal gain, and to

[80] The Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, Art. 3.
[81] I. Zinovkina, Cybersecurity in 2023–2024: Trends and Forecasts [*Kiberbezopasnost' v 2023–2024 gg.: trendy i prognozy*] (in Russian), 12 December 2023. https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/?utm_source=tg_pt&utm_medium=post&utm_campaign=2023_2024&utm_content=12_14 (accessed 13 September 2024).
[82] ibid.
[83] Bill No. 502104-8 "On Amendments to the Code of the Russian Federation on Administrative Offenses". https://sozd.duma.gov.ru/bill/502104-8 (accessed 10 September 2024).
[84] Bill No. 502113-8 "On Amendments to the Criminal Code of the Russian Federation". https://sozd.duma.gov.ru/bill/502113-8 (accessed 10 September 2024).

combat the 'black market' of personal data.[85] That said, the initiative raises serious concerns among IT companies: such a serious tightening of responsibility might lead to a significant slowdown in the development of AI which uses large amounts of data; besides, the current wording of the bill on amendments to the Criminal Code can be interpreted in such a way that their effect extends not only to wrongdoers, but also to the owners and management of IT companies that collect Big Data from open sources and use it for their own developments.[86] The issue of the development of neural networks and Big Data was raised repeatedly during discussing the bill in parliament; however, it seems that the protection of personal data is a higher priority for the legislator at the current stage of regulation design in this area.

In line with this priority, in December 2022 the Federal Law was adopted on the procedure for collecting and processing biometric data and creating a unified system of biometric data.[87] The law indicates facial image and voice sample as the only types of biometric data to be collected[88] and prohibits collection of genomic information;[89] establishes a mechanism for a person to check information about her previously given consent to the processing of biometric data, as well as all actions performed with her biometric data[90] and provides for the right of a person to revoke her previously given consent to the processing of her biometric data at any time;[91] and prohibits cross-border transfer of collected biometric data.[92] Also, in accordance with the law, biometric data will be collected and processed using the Unified Biometric System (the 'UBS'). Commercial and government organizations are obliged to transfer the biometric data (photos and voice samples) accumulated before the law came into force to the UBS. Thus, as a general rule the biometric data cannot be collected and stored in other information system then the UBS.[93] Commercial organizations can obtain information from the UBS by concluding a special agreement with the operator of the UBS. Banks still have the right to collect biometric data, but they are obliged to

[85] E. Yasakova, A bill to Toughen Penalties for Data Leaks Introduced to the State Duma [*V Gosdumu vnesli zakonoproekt ob uzhestochenii nakazanija za utechki dannyh*] (in Russian), RBC (4 December 2023). https://www.rbc.ru/technology_and_media/04/12/2023/656b79229a7947016853c8ff (accessed 10 September 2024).
[86] T. Isakova, Big data Gets Excited Before Deadline [*Bol'shie dannye vzvolnovalis' do sroka*] (in Russian). Kommersant (8 December 2023). https://www.kommersant.ru/doc/6382087 (accessed 10 September 2024).
[87] Federal Law dated 29 December 2022 No. 572-FZ "On the Implementation of Identification and (or) Authentication of Individuals Using Biometric Personal Data, on Introducing Amendments to Certain Legislative Acts of the Russian Federation and Invalidating Certain Provisions of Legislative Acts of the Russian Federation".
[88] ibid, Art3(4).
[89] ibid, Art 3(8).
[90] ibid, Art 3(14).
[91] ibid.
[92] ibid, Art 3(21).
[93] ibid, Art 4.

transfer all collected data to the UBS so that it can be encrypted and returned to facilitate interaction with clients in the form of identifiers.[94]

3.2. Focus on AI as the game-changer in the digital transformation

In Russia, the vector for the legal regulation of AI has been determined by a number of strategic planning documents most of them being in the form of a decree (*ukaz*) of the President or a resolution (*postanovlenie*) of the Government. In particular, the President approved the "National Strategy for the Development of Artificial Intelligence for the Period until 2030"[95] (the 'AI National Strategy'), and the Government adopted the "Concept for the Development of Regulation of Relations in the Field of Artificial Intelligence Technologies and Robotics for the period until 2024".[96] Both these documents are pieces of subordinate legislation; in the absence of a comprehensive federal law regulating the use of AI, the lack of unified legislative definition and conceptual construct indicates the initial stage of legislative regulation of this area. Herewith, alongside the state documents of strategic planning, there is a substantive and significant document of self-regulation, developed with the participation of key industry players joining their efforts in the AI Alliance Russia[97] — the AI Ethics Code which contains guiding principles. They include respect for human autonomy and free will, non-discrimination, and identification of AI in communication with humans, and aims at creation of tools for interaction between the Government, developers, scientific organizations and the society to enhance ethical and responsible development, implementation and use of AI technologies.[98] Adherence to the AI Ethics Code is voluntary; currently there are more than 270 signatories to the Code, including major IT companies, research institutions and civil society organizations.

The path of transformation of legal regulation from strategic documents, individual industry regulation and self-regulation acts to full-fledged legislation corresponds global trends in

---

[94] ibid, Art 4(7).

[95] Decree of the President of the Russian Federation dated 10 October 2019 No. 490 "On the Development of Artificial Intelligence in of the Russian Federation" as amended by the Decree of the President of the Russian Federation dated 15 February 2024 No. 124. The national strategy of the AI development was prepared with active participation of Sberbank – the major bank in the Russian Federation and CIS, 50% plus 1 share in the capital of which is owned by the state-controlled National Welfare Fund of Russia.

[96] Decree (*rasporyazhenie*) of the Government of the Russian Federation dated 19 August 2020 No. 2129-r "On Approval of the Concept for the Development of Regulation of Relations in the Field of Artificial Intelligence Technologies and Robotics for the Period until 2024".

[97] Founded in 2019, the Alliance brings together leading technology companies such as Yandex, VK, Sber, Russian Direct Investment Fund, to jointly develop their competencies and accelerate the implementation of artificial intelligence in education, scientific research and practical business activities. The main task of Alliance is to monitor the implementation of the AI Strategy. For more details, visit https://a-ai.ru/?lang=en (accessed 14 September 2024).

[98] The AI Ethics Code is available in English at https://ethics.a-ai.ru/assets/ethics_files/2023/05/12/AI_ETHICS_CODE_10_01_1.pdf (accessed 14 September 2024).

the development of the AI regulatory framework, in particular in the USA, China and the European Union. Although an all-embracing federal law on AI has not yet been developed in Russia, documents already adopted support the analysis of the proposed approaches for further development of relevant legislation.

Thus, the AI National Strategy was significantly amended in February 2024, in particular to clarify the AI terminology.[99] It defines AI as a set of technological solutions that allows one to imitate *human cognitive functions* (including self-learning and searching for solutions without a predetermined algorithm) and obtain results when performing specific tasks that are *comparable, or superior, to the results of human intellectual activity*; the set of technological solutions includes information and communication infrastructure, software (including those that use machine learning methods), processes and services for data processing and finding solutions.[100] Evidently, this definition is based on the correlation between AI and natural human intelligence (although such a definition as 'imitation of human cognitive functions' allows for many interpretations — for example, whether the implementation of a simple mathematical operation with an ordinary calculator is an imitation of human cognitive functions) and is not limited to the technical characteristics of AI as an algorithm or a self-learning system. Moreover, one can note a very broad scope the definition: it covers all currently known forms of AI. Besides, amendments to the AI Strategy of February 2024 introduced definitions of 'large generative models', 'strong artificial intelligence', 'artificial intelligence model', 'trusted technologies of artificial intelligence' and several others.[101]

The AI Strategy also notes that Russia has significant potential to become one of the international leaders in the development and use of AI due to a high level of physics and mathematics education, a strong natural science school (largely inherited from the Soviet period), and the presence of competencies in modelling and programming.[102] Accordingly, support for scientific research and increasing the level of provision of the Russian AI technology market with qualified personnel are highlighted among the primary tasks formulated in the AI Strategy. Herewith, the burden of financing the AI Strategy implementation falls on the state: it is carried out at the expense of the federal budget, funds from so called extra-budgetary sources, including funds from development institutions, state corporations, state-owned companies, joint-stock

[99] Decree of the President of the Russian Federation dated 15 February 2024 No. 124.
[100] AI National Strategy, Art 5(a), emphasis added.
[101] Decree of the President of the Russian Federation dated 15 February 2024 No. 124, Art 3(g).
[102] AI National Strategy, Art 13.

companies with state participation.[103] In fact, funding for the federal AI project continues to increase despite the difficulties that the Russian budget is experiencing in the face of sanctions and extraordinary military spending: thus, in October 2023, the government allocated an additional 1.2 billion rubles ($13.3 million) to support AI-related developments, including small businesses – developers of products and services based on AI.[104] Spending on the national project 'Artificial Intelligence' in the federal budget plan for 2025-2027 continues to rise, even amid unprecedented military spending: a total of 3.9 billion rubles ($43 million) of federal funds are allocated for the development of AI for the next three years.[105] The volume of private investment attracted to finance AI in Russia remains limited.[106] To reduce this gap and support the venture capital market, the Ministry of Economic Development proposes to use system-wide measures to support the 'Take Off - from Startup to IPO' strategic initiative: in particular, allow individuals to participate in investment partnerships (currently these are only commercial organizations and individual entrepreneurs),[107] reduce the tax burden of investors, take into account unsuccessful investments when calculating taxes, and prepare the portfolio assessment of the financial result.

An important feature of AI Strategy is that the use of AI technology is defined within the civilian sphere and the scope of national economy, while excluding military use. This strategic plan specifically points to the development of the Russian AI market, although AI technology is certainly (and not least) developing in modern Russia specifically for military use as will be discussed in more detail later in this section.

In practical terms, the AI technologies are most actively used in providing public services — particularly, many AI solutions are implemented in the work of the *Gosuslugi* portal. At the same time, application of AI is not limited to the provision of public services (although the importance of AI technology in this area can hardly be overestimated), but in many other areas, both military and civilian. AI technologies are integrated into the space industry. Machine learning methods are used in the field of the Earth remote sensing: in August 2023, Terra Tech neural

[103] AI National Strategy, Art 55
[104] Decree of the Government of the Russian Federation dated от 5 October 2023 No. 2715-r.
[105] What digital expenditures are included in Russia's draft budget for 2025-27 [*Kakie cifrovye rashody zalozheny v proekte bjudzheta Rossii na 2025-27 gg*] (in Russian), Digital Russia (1 October 2024). https://d-russia.ru/kakie-cifrovye-rashody-zalozheny-v-proekte-bjudzheta-rossii-na-2025-27-gg.html (accessed 12 October 2024).
[106] Avenger, Thoughts on Russia's National Artificial Intelligence Strategy' [针对俄罗斯国家人工智能战略的思考] (in Chinese), 51CTO (21 June 2020). https://ai.51cto.com/art/202006/619342.html (accessed 14 September 2024).
[107] Department of Strategic Development and Innovation of the Ministry of Economic Development of the Russian Federation, 'More than 100 High-Tech Companies Received Preferential Financing During the Year under the "Take Off - from Startup to IPO" Program' (13 April 2023). https://www.economy.gov.ru/material/news/bolee_100_vysokotehnologichnyh_kompaniy_poluchili_za_god_lgotnoe_finansirovanie_po_programme_vzlet_ot_starta_do_ipo.html (accessed 14 September 2024).

network solutions based on satellite imagery data and AI were presented at the International Forum on Artificial Intelligence for Business.[108] Terra Tech for the first time demonstrated the digital map of Russia's economic activity, formed on the basis of the analysis of space imagery data within the framework of the "Digital Earth – Services" project. Geo-solutions applicable to managing farmland and monitoring land desertification were also presented. Other areas of application of the AI technologies in the space systems and complexes include neural networks and other technologies to address the processing of large amounts of heterogeneous satellite information, including onboard processing; multi-agent technologies of autonomous control of multi-satellite orbital groups; intelligent systems to support the model-oriented design of space systems and their components; robotic devices designed to service spacecraft in orbit and solve other problems.[109]

Among other initiatives to employ AI solutions for civilian purposes, the regulatory sandbox in Moscow is worth noting. The areas for the experimental use of AI include diagnosing cancer using MRI images, speech recognition for processing incoming calls regarding municipal services to citizens, video recognition, electronic voting and autonomous vehicles. Now the 'regulatory sandbox' operates on the basis of the Federal Law[110] establishing a five-year (2020 – 2025) experiment for the development and implementation of AI in Moscow, including allowing AI systems to process anonymized personal data for governmental and certain commercial business activities. AI technology is most widely used in healthcare technologies. Moscow has been digitalizing its healthcare system for more than ten years. Now this process is based on a single digital platform, which is developed by the Moscow Department of Information Technology. In particular, at the Center for Diagnostics and Telemedicine[111] of the Moscow Department of Health, an experiment is being conducted to introduce computer vision technologies into medicine. Since 2020, within this experiment more than 11 million medical images across 28 clinical areas have been analysed using computer vision technology. Among them are lung cancer, pneumonia, osteoporosis, aortic aneurysm, coronary heart disease, stroke,

[108] Russian Space Systems, Artificial Intelligence Transforms Space Geotechnologies (17 August 2023). https://russianspacesystems.ru/2023/08/17/iskusstvennyy-intellekt-transformiruet/ (accessed 14 September 2024).
[109] A. N. Balukhto, A. A. Romanov, Artificial Intelligence in Space Technology: State, Development Prospect [*Iskusstvennyj intellekt v kosmicheskoj tehnike: sostojanie, perspektivy razvitija*] (in Russian), Rocket and Space Instrument Engineering and Information Systems 6(1) (2019). https://russianspacesystems.ru/wp-content/uploads/2019/04/8_p65_0601.pdf (accessed 12 September 2024).
[110] Federal Law dated 24 April 2020 No. 123-FZ "On Conducting an Experiment to Establish Special Regulation in Order to Create the Necessary Conditions for the Development and Implementation of Artificial Intelligence Technologies in the Subject of the Russian Federation - the City of Federal Significance Moscow and Amendments to Articles 6 and 10 of the Federal Law 'On Personal Data".
[111] The Center for Diagnostics and Telemedicine. https://telemedai.ru/en/o-nas (accessed 12 September 2024).

pulmonary hypertension, hydrothorax.[112] Six comprehensive AI solutions in the pilot project search for up to 10 pathologies simultaneously in one examination of the chest and abdominal organs. Smart algorithms are available to radiologists in 150 city hospitals.

As indicated above, the AI Strategy, as well as federal legislation on regulatory sandboxes, addresses the use of AI technologies for civilian purposes, in particular in medicine, the financial sector, and the provision of public services in a broad sense. At the same time, application of AI in warfare has also been the focus of government and military experts over the past few decades, and in the last five years this issue has become one of the central topics in discussions. Thus, since 2018 the Ministry of Defence held annual conferences on application of AI for military purposes, while development of AI is listed among priority research areas for national security.[113] In 2022, a department for the development of AI was created within the Russian Ministry of Defence to intensify work on the use of these technologies in the development of weapons.[114] In July 2022, Defence Minister Shoigu approved the Concept of the activities of the Armed Forces of the Russian Federation in the development and use of weapons systems using AI technologies (restricted document).[115] Military AI applications integrate many systems managing the means of attack, control, and intelligence. Due to the involvement of the Ministry of Defence in the research and application of AI, related achievements are closely correlated with military interests and have a high degree of confidentiality, which complicates obtaining comprehensive and accurate information and analysis of the state of AI development in this sector.[116]

The capabilities of the AI technology are also used to ensure investigation tasks, which, like the entire national security discourse, have been on the agenda especially acutely over the past

---

[112] In Moscow, Artificial Intelligence Increased the Speed and Accuracy of Radiology Diagnostics [*V Moskve iskusstvennyj intellekt povysil skorost' i tochnost' luchevoj diagnostiki*] (in Russina), Mos.ru (18 November 2023). https://www.mos.ru/news/item/132247073/ (accessed 12 September 2024).

[113] Ministry of Defence of the Russian Federation, Conference "Artificial Intelligence: Problems and Solutions - 2018 [*Konferencija "Iskusstvennyj intellekt: problemy i puti ih reshenija — 2018"*] (in Russian). https://mil.ru/conferences/is-intellekt.htm (accessed 12 September 2024).

[114] Department for Artificial Intelligence Created in the Ministry of Defence of the Russian Federation [*V Minoborony RF sozdali upravlenie po rabote s iskusstvennym intellektom*] (in Russian), TASS (17 August 2022). https://tass.ru/armiya-i-opk/15492531 (accessed 12 September 2024).

[115] Ministry of Foreign Affairs of the Russian Federation, Commentary by Russian Foreign Ministry Spokesperson M.V. Zakharova on the Activities of the Group of Governmental Experts of States Parties to the Convention on Certain Conventional Weapons on Lethal Autonomous Weapons Systems [*Kommentarij oficial'nogo predstavitelja MID Rossii M.V.Zaharovoj o dejatel'nosti Gruppy pravitel'stvennyh jekspertov gosudarstv-uchastnikov Konvencii o «negumannom» oruzhii po smertonosnym avtonomnym sistemam vooruzhenij*] (in Russian), (23 August 2022). https://www.mid.ru/ru/foreign_policy/news/1827203/ (accessed 12 September 2024).

[116] For the review of Russian bibliography on AI integration in the systems of command over nuclear weapon refer, e.g., to: O. Shakirov, Russian Thinking on AI Integration and Interaction with Nuclear Command and Control, Force Structure, and Decision-Making, European Leadership Network (13 November 2023). https://www.europeanleadershipnetwork.org/report/russian-thinking-on-ai-integration-and-interaction-with-nuclear-command-and-control-force-structure-and-decision-making (accessed 14 September 2024).

few years. One of the major areas of such application is video surveillance, particularly in the city of Moscow within the 'Safe City' project. The facial recognition capability of cameras has proven its effectiveness in identifying and searching for suspects in administrative offenses and crimes: the RFS 'Sphere' (*Sfera*) for 2.5 years from the beginning of its use in the Moscow metro in September 2020 and until March 2023 helped detect 6012 people suspected of committing crimes.[117] Herewith, application of the FRS is an ongoing concern from the standpoint of the protection of human rights (in particular, privacy) and, in general, possible abuses by law enforcement agencies. In particular, advanced video surveillance and FRS was used in Moscow to detain participants in political protests in 2021 and anti-mobilization protests in 2022.

On 4 July 2023 the European Court of Human Rights issued a ruling on the case *Glukhin v. Russia*.[118] The Court held that the use of FRS to identify a single-person picket participant and later to locate and arrest him while he was travelling in the Moscow metro violates the right to respect for his private life and freedom of expression.[119] The applicant, a Russian political activist, was detained in Moscow metro in 2019 as he was identified by FRS in the video cameras installed in the Moscow metro as a participant of a single-person picket which took place two days before the detention. The screenshots of a public Telegram channel with photographs and a video of the single-person picket, as well as the video-recordings from the metro surveillance cameras were subsequently used in evidence in the administrative-offence proceedings against the applicant.[120] The Russian Government did not deny that the FRS was used to identify and arrest the applicant but claimed that he had committed an administrative offence (a single-person picket without prior notification) and that all the operational-search measures taken against him by the police had been lawful and justified.[121] The Court, however, concluded that Russian legal provisions on the processing of biometric personal data are broadly formulated and do not contain "any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or on processing of sensitive personal data".[122] Moreover, the applicant was not provided with any procedural safeguards with

[117] Facial Recognition System in the Moscow Metro Helped Police Find 6,012 Suspects [*Sistema raspoznavanija lic v metro Moskvy pomogla policii najti 6012 podozrevaemyh*] (in Russian), Interfax-Russia (29 March 2023). https://www.interfax.ru/moscow/893460 (accessed 12 September 2024).
[118] *Glukhin v. Russia* App no 11519/20 (ECtHR, 4 July 2023). Federal Law dated 11 June 2022 No. 183-FZ allowed the Russian government not to implement ECtHR decisions taken after 15 March 2022, the day the Russian Federation left the Council of Europe. Despite this, the ECtHR continues to consider complaints from Russian citizens if violations of the ECHR occurred before 16 September 2022.
[119] ibid, paras 73, 88.
[120] ibid, para 68.
[121] ibid, para 62.
[122] ibid, para 83.

respect to processing his personal data with the use of FRS, such as prior court authorisation of surveillance, supervisory control or available remedies.[123] Finally, as the applicant was accused of a minor administrative offence, not a crime, the use of live FRS to locate and arrest him in the Moscow metro did not correspond to a 'pressing social need'[124] and, in general, "could have a chilling effect in regard of the rights to freedom of expression and assembly".[125]

As AI technologies develop, more and more questions arise in the field of legal regulation of this area. One of the most pressing among them is the implementation of the 'data sanitization' procedure, which allows to transform databases that have signs of personal data into safe ones that can be used for the development of AI. At the end of June 2023, the Russian Ministry of Digital Development announced the formation in 2024 within its information system of a specialized center based on the National Technology Center for Digital Cryptography for the anonymization of personal data of citizens, that is, transforming them in such a way that it is impossible to attribute them to a specific person.[126] The creation of such a center and the implementation of this anonymization procedure will require amendments to the federal legislation on personal data.

Regulating accountability for the harm caused by AI is equally important. The question of who is responsible for the harm caused by AI, given that the technology is self-learning and at various stages of its development is taught not only by those who create it, is relevant for all jurisdictions investing in the development of AI technology. The Russian legislator will have to develop an approach to solving the problem of liability for harm caused by AI systems, also considering the need for a balance between regulation and ensuring sufficient freedom to maintain pace of development and implementation of technological solutions.

Altogether, development and implementation of AI technologies is considered by the Russian government as one of the key tasks, the achievement of which is generously financed from the budget. Approaches to regulating AI remain rather cautious so as not to impede the development of technology — at the Sberbank conference on artificial intelligence 'AI Journey', the Russian President formulated an intention to make Russia one of the most comfortable jurisdictions in the world for the development of AI.[127] At the same time, the practice shows that

[123] ibid.
[124] ibid, para 89.
[125] ibid, para 88.
[126] A Center for Anonymizing Data for AI Training Will Be Created in Russia [*V Rossii sozdadut centr obezlichivanija dannyh dlja obuchenija II*] (in Russian), RIA (28 June 2023). https://ria.ru/20230628/mintsifry-1880808955.html (accessed 13 September 2024).
[127] Putin Spoke About the "Cancellation" of Russia in the Digital Space [*Putin rasskazal ob «otmene» Rossii v cifrovom prostranstve*] (in Russian), RBC (24 November 2023). https://www.rbc.ru/technology_and_media/24/11/2023/6560ae4e9a794723244cfffd (accessed 13 September 2024).

the main areas of the AI application are support for the public sector (in a broad sense, including search activities and surveillance of citizens, controversial from the standpoint of respect for their constitutional rights) and the military.

Conclusion

The paper examines certain aspects of the process of digital transformation in Russia from the early 2000s, when digital initiatives aimed at the increase in the efficiency of government functions and facilitation of more accessible, speedy and convenient receipt of government services, until the present crisis time of post-COVID-19 and Russia's military operation in Ukraine. The government transformation process has had its ups and downs from the initial stages to the present day.[128] The first E-Government Survey in 2003 placed the Russian Federation 58th out of 193 states with the E-Government Development Index lagging more than twice as far behind the then world leader, the USA.[129] The situation improved significantly in 2012, when Russia moved up to the 27th place from 59th position in the previous survey in 2010 and became the sub-region leader. In all probability, this jump was caused by the launch of the unified federal portal of state services *Gosuslugi* during this period. The situation stagnated in the following years and has worsened since 2020; according to the latest 2022 survey, Russia, although still being designated a state with a very high E-Government Development, ranks only 42 out of 193.[130]

Returning to the theories of the government digitalization discussed at the beginning of this paper, it can be noted how different approaches are combined within the same state at different stages of the digitalization process. The initial motivation for the development of e-government in Russia can probably be categorised as falling under the scope of the *systems* theory with a focus on creation of advanced IT infrastructure of digital government and increasing the convenience for citizens in interaction with government agencies. This task, as was discussed in relation to the work of the *Gosuslugi* service, was successfully solved. Herewith, from the mid-2010s until today, the digitalization process has been taking place more in the logic of the *reinforcement* and *legitimation* theories, with special attention paid to the tasks of the state and 'sovereignization' of the national Internet segment. It is noteworthy that this change coincides with the introduction of the concept of 'cultural sovereignty' (as separation from the West) and 'traditional values'[131] (in

[128] See, e.g.: M. Zherebtsov, Taking Stock of Russian e-Government, Europe-Asia Studies 71 (2019) 1–29.
[129] UN E-Government Knowledgebase, Russian Federation. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/141-Russian-Federation/dataYear/2003 (accessed 13 September 2024).
[130] UN E-Government Knowledgebase, Russian Federation. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/141-Russian-Federation/dataYear/2022 (accessed 13 September 2024).
[131] M. Rudnev, Traditional Values and Reality [*Tradicionnye cennosti i real'nost'*] (in Russian), Vedomosti (17 May 2019). https://www.vedomosti.ru/opinion/articles/2019/05/16/801630-traditsionnie-tsennosti (accessed 13 October 2024).

contrast to the 'imposed Western values') into the Russia's political narratives as a reflection of neoconservatism — Russian cultural norms are declared of being under attack by external and internal forces causing a sense of 'ontological insecurity'.[132] Reflecting this growing sense of insecurity, also shaped by the official state rhetoric, is a change in the Russian population's perception of the values of security/order and freedom. The widely cited World Values Survey showed that in the period 2017-2020 (the last period when the study was conducted in Russia), 72% of respondents considered security more important than freedom.[133] For comparison, in the survey of 1995, 51,5% of respondents named respect for freedom of the individual as the most important responsibility of the government, while 42.4% considered maintenance of order in society to be the most important.[134]

The digital transformation process has notable positive effects, such as the creation of a convenient and effective platform for the provision of public services *Gosuslugi*, the development of specialized legislation (for example, on the protection of biometric personal data), state programs for the development of AI generously financed from the budget, as well as measures for the development of national software that contribute to the development of Russian IT companies and the industry as a whole. At the same time, digitalization today is carried out to a much greater extent in the interests of the state being justified with the need to ensure national security and the technological sovereignty. Signs of this shift to a state-centric digitalization model are the expansion of the powers of supervisory authorities (including, the powers of *Roskomnadzor* to block the traffic), the introduction of new registration databases with the accumulation of data on citizens and the use of modern technologies such as AI and facial recognition to enhance control over Russians. The Sovereign RuNet Law also indicates a tendency towards digital autarchy. It can be assumed that these phenomena are part of a broader political, social and cultural process of disengagement that Russian society is currently undergoing, including under the influence of official rhetoric about threats to 'ontological security'.

[132] F. Prina, Fantasies of cultural sovereignty and national unity: Russia's ontological (in)security and its assertion of 'spiritual-moral' values. International Politics, 2024. https://doi.org/10.1057/s41311-024-00600-w (accessed 14 September 2024).
[133] C. Haerpfer, R. Inglehart, A. Moreno, C. Welzel, K. Kizilova, J. Diez-Medrano, M. Lagos, P. Norris, E. Ponarin, B. Puranen (Eds.). 2022. World Values Survey: Round Seven – Country-Pooled Datafile Version 6.0. Madrid, Spain & Vienna, Austria: JD Systems Institute & WVSA Secretariat. Report on the Russian Federation, available at: https://www.worldvaluessurvey.org/WVSDocumentationWV7.jsp (accessed 14 September 2024). P. 49.
[134] R. Inglehart, C. Haerpfer, A. Moreno, C. Welzel, K. Kizilova, J. Diez-Medrano, M. Lagos, P. Norris, E. Ponarin, B. Puranen et al. (Eds.). 2014. World Values Survey: Round Three. Report on the Russian Federation, available at: https://www.worldvaluessurvey.org/WVSDocumentationWV3.jsp (accessed 14 September 2024). P. 36.