Problems and Risks of Digital Transformation in Russia

V. V. Moiseev[1], A. P. Kochetkov[2] and V. I. Borisovsky[1]
[1]*Belgorod State Technological University named after V. G. Shukhov, Kostyukova St, 46, Belgorod, Russia*
[2]*Moscow state University named after Lomonosov, Moscow, Russia*

Keywords: information technology, digital transformation, digital society, government bodies, risks.

Abstract: The use of information technology is of great importance for increasing the competitiveness of the economy and increasing the efficiency of government bodies. Speaking about information technologies of public administration, it should be understood that, first of all, we are talking about the informatization of all administrative processes in government bodies of all levels, about informatization of interdepartmental relationships, about the creation of computer systems capable of supporting all the functions of interaction of these bodies with the population and business structures. The political course adopted in 2017 towards the formation of a "digital society" presupposes the need for a fundamental understanding of the processes of digital transformation of the economy, power communications and political relations in the context of global challenges and domestic socio-cultural traditions, with the aim of their effective implementation into domestic political practice. In the context of the global trend towards total digitalization of all socio-political relations, it is necessary to develop specific mechanisms for effective public administration based on new technologies in the interests of the entire Russian society. Today, the concept of "smart city" or smart city is also extremely popular, the implementation of which is carried out not only in Russia, but also in many countries of the world. Without rejecting the positive potential of Russia's digital transformation, we note a number of problematic issues and risks associated with this concept.

1 INTRODUCTION

Modern society is characterized by a global process of digitalization of social and economic relations.

Today, the future of the world community largely depends on the new technological order in the information space in all spheres of political, economic, social and public activity. In this regard, the role of law, the key mechanism for regulating social relations, is sharply increasing. Practice has shown that digital transformation and the information society are developing so rapidly that the current legislation is not able to adequately influence the ongoing processes. Therefore, legal systems require fundamental changes. First of all, it is necessary to redefine such categories as law, offenses, legal responsibility in relation to the new digital space.

The concept of "digital government" began to form in political science as a result of the evolution of the earlier model of "e-government", which gradually exhausted its heuristic potential. The development of the concept of "electronic government" began at the turn of the XX-XXI centuries. in response to the current challenges of the time associated with the need to introduce innovative digital, intelligent technologies into the system of political management in order to improve its quality and efficiency through the provision of public services in electronic form and more efficient use of information flows in the management system. Gradually, the main areas of research were formed, including: electronic government services; organization and political management; infrastructure, integration and interoperability; knowledge and information management; Information Security; civil initiatives and voting; mobility of services and operations; archiving, electronic accounting and document lifecycle management (Delcambre, 2005). From the very beginning, research in the field of e-government was interdisciplinary, combining political science, public administration, communication, and management. In political science, the initial focus of e-government research was on the use of Internet technologies in political governance for the purpose of providing public services and developing democracy. In this regard, the definition of e-government, given by the American political scientist

Moiseev, V., Kochetkov, A. and Borisovsky, V.
Problems and Risks of Digital Transformation in Russia.
DOI: 10.5220/0010683700003169
In *Proceedings of the International Scientific-Practical Conference "Ensuring the Stability and Security of Socio-Economic Systems: Overcoming the Threats of the Crisis Space" (SES 2021)*, pages 88-94
ISBN: 978-989-758-546-3

D. West, is quite representative, as “the use of the Internet and other digital means by public authorities for the provision of public services and information, as well as the implementation of democracy” (West, 2005). In this regard, we note the monograph of the famous English researchers from Cambridge A. Brown, J. Fishenden and M. Thompson "Digital Government" (Brown, 2014) as well as the collective monograph of researchers from the University of Granada (Spain), ed. prof. Laura Munyas and Pedro Rodriguez Bolivara "International experience in the development of electronic government" (Alcaide, 2018).

The influence of socio-cultural traditions on digitalization processes was especially vivid in China, where the national mentality, geographic and demographic characteristics became a serious brake on the path of digital transformation of society. Many researchers note that e-government technologies are often used here to demonstrate the conformity of reforms to world experience, and not as an effective tool for reforms (Lovelock, 2013). The share of Russians with digital literacy has increased from 26% in 2018 to 30% in 2020 (NAFI, 2020). According to the Foundation's data, public opinion 22% of Russians have never used the Internet in their life (NEWSru, 2020).

The analysis of user activity in social networks suggests that in most cases Internet users prefer the products of such giants as Google, Facebook, YouTube, which indicates the dominance of monopolies in the information services market. And the hegemony of large companies is direct evidence of the authoritarianism reigning in the field of information policy. To protect your national sovereignty, it is necessary to carry out the sovereignty of the Internet. Therefore, in Russia, a law on "sovereign Internet" was adopted and came into force in November 2019 in Russia (RBC, 2021). All this poses a serious problem about the formation of an elite digital democracy, in which the elite will have a special character. Its high status will be determined not by the previous criteria - wealth, education, closeness to power, but by access to technologies and the availability of experience in using them. The very selection of a certain group of Internet users who are more ready than others to participate in political life will become a problem for real democracy. This netocratic elite is getting out of the control of the citizens, because no one delegates to it the authority to manage on the basis of procedures recognized in society (Alcaide, 2018). Therefore, the question arises: will digital democracy be so democratic in general, based on the will and activities of the most active Internet users?

It is also impossible to exclude falsification of the results of sociological polls and voting by the state apparatus. Bribery of certain social groups can be very likely to create a false public opinion. Since not all Russian citizens use the Internet, it is possible to divide society into citizens who have information and those who do not have access to it.

One cannot ignore the fact that the development of digital democracy has not yet led to a significant increase in the political activity of citizens. It is also important to note that with broad access of citizens to online electoral systems, users who have anti-state or anti-constitutional opinions may become more active. There is no guarantee that the majority of good citizens will be active in online electronic communication. Digital transformation has the potential to lead to new forms of “abuse” of power, such as the use of digital media to impose policy decisions from the “top”, as digital democracy can be used to maintain and exacerbate inequalities between those who have access to the Internet and those who have access to it. deprived.

Experts raised the issue of digitalization as a new system of total surveillance of citizens based on an analysis of their Internet activities and the dangers of society “programming”. A particular danger of this control system lies in its veiled nature: access to algorithms that ensure the functioning of much-needed recreational and communication services, online banking systems, allows the state, business structures and hackers to freely violate, for example, the right to privacy.

In our country, there are also certain socio-cultural barriers to digital transformation. Therefore, it is necessary to take into account the influence of the mentality and socio-cultural traditions, geographical factors, the level of human capital development, and the influence of subjective factors. It is especially worth paying attention to the uneven economic and demographic development of the regions on the scale of our huge country: the different level of digitalization in the field significantly complicates the transition to a new model of "digital government", increases political risks (Kochetkov, 2020).

The experience of modern modernization in Russia convincingly demonstrates that the domestic bureaucracy is quite conservative and is interested in further preserving its state. The bureaucratic resistance to reform is particularly pronounced in remote regions, where innovation is mainly approached formally in order to publicly demonstrate the presence of new fashion trends, rather than using

innovation as an effective tool for transforming the system of political governance.

In the context of assessing the political risks of the digitalization of power, these are very alarming signals: there are obvious contradictions between the federal government, which seeks to form an open government, and the regional government, which essentially hinders this initiative. For example, modern sociological studies in the regions of Russia have shown that at present local authorities in Russia do not strive for openness to citizens, bilateral communications between the administration and civil society are poorly developed, there is a low level of public awareness of new programs and public initiatives, electronic hearings and sociological surveys are very rarely conducted.

It is also important to recall the negative aspects of the digitalization of power in foreign countries, especially in Singapore, where the lack of dialogue with civil society has led to the formation of information totalitarianism. It is important to take into account these political risks of the development of information totalitarianism when conducting a national digital transformation (SecurityLab, 2017).

It should be emphasized that the domestic model of "digital government" must necessarily include control by civil society, active participation of citizens in the decision-making process, and mandatory electronic voting on key public issues. A very important task on the path of digitalization of Russian society is the formation of a modern level of culture of digital communications and openness of the authorities throughout the country.

Currently, the insufficiently qualified level of both civil servants and citizens, and their often negative attitude towards digital technologies, are serious political risks and a brake on the path of reform. As long as there is a significant layer of people in Russian society who do not possess digital technologies and are not able to use digital technologies from beginning to end, it is impossible to move to a new management model. That is why it is important to launch digital technology training programs in all regions of Russia today, so that citizens can take advantage of the "digital society" and "digital government"in the near future.

With digital transformation, it is important to pay attention not only to the digitalization of power, but also to the development of human capital, the level of digital culture of the entire civil society. It is well known that the effectiveness of management models depends, first of all, on a person, and not on technology. Any most modern technologies become ineffective over time, and a person strives to develop, to go forward to new heights, using and increasing his knowledge, abilities and competencies

All this poses a serious problem about the formation of an elite digital democracy, in which the elite will have a special character. Its high status will be determined not by the previous criteria - wealth, education, closeness to power, but by access to technologies and the availability of experience in using them. The very selection of a certain group of Internet users who are more ready than others to participate in political life will become a problem for real democracy. This non-theocratic elite is getting out of the control of the citizens, because no one delegates to it the authority to manage on the basis of procedures recognized in society (Legal social network 9111, 2019). Therefore, the question arises: will digital democracy be so democratic in general, based on the will and activities of the most active Internet users, while the majority of the electorate is passive? It is also impossible to exclude falsification of the results of sociological polls and voting by the state apparatus. Bribery of certain social groups can be very likely to create a false public opinion. Since not all Russian citizens use the Internet, it is possible to divide society into citizens who have information and those who do not have access to it.

Thus, today the problem of openness of the central and regional authorities to dialogue with the public has become very acute, and until we solve this problem, the digital transformation of Russia will be slowed down, and the risks of information distortion will increase.

2 MATERIALS AND METHODS

In the article, the authors used analytical, comparative, statistical and institutional methods of a systematic approach to the study of this problem.

The authors made an attempt, on the basis of the listed research methods, to reveal the true situation in the digital transformation of Russian society, to identify the main problems and risks associated with these processes taking place in modern Russia.

The materials for the article were official documents of the head of state and government of Russia, statistical data, monographs and scientific articles by leading Russian scientists.

3 RESULTS AND DISCUSSION

Recently, the authors of this article got acquainted with an interesting study of the American professor, director of the Laboratory of Management at New York University Beth Simone Novek, a former adviser to US President Donald Trump (Novek, 2016). She argues that a smart state largely depends on a smart population that actively uses digital technologies both in the economy and in the social sphere and in everyday life. At the same time, Simona Novek argues that the digital transformation of socio-economic processes will dramatically improve the quality and standard of living of Americans. In principle, almost everything is true, except, perhaps, one most important factor: how the state will use the achievements of digital civilization - for the good or to the detriment of its citizens, or will it combine both, implementing the "carrot and stick" policy. It is obvious that information technologies can be used in different ways: both for general prosperity and development of civil society, and for total surveillance of citizens, massive fines based on the results of photo and video recording from cameras, which are abundantly installed on the country's roads. The attempts of the tax inspectorate to control the bank accounts of citizens, violating bank secrecy, can be viewed in the same vein. Not to mention the actions of numerous special services and law enforcement agencies, which, without court sanction, are spying on Russians, ranking them as unreliable people. In addition, if these days authorities are not acting in good faith when they hack into our devices, and the Internet allows us to fall prey to the onslaught of targeted advertising, then how will we protect our data in the future?

Face recognition using IT technologies and robots based on powerful processors does not mean that we will be constantly monitored, as in the case of drones that are already used for video control? These and other innovations related to digital transformation are already being used by government agencies for total surveillance of citizens: video surveillance cameras are installed not only on highways, but also on city streets, in supermarkets, at stadiums, and in other places where citizens gather. It is known that digital technologies make it possible to track citizens not only in offices, but also in their homes and apartments using webcams, smartphones, and other gadgets and devices. These technologies allow the creation of data about us without our permission, and we have no control over it. All of this paints eerie comparisons with Orwell's "Big Brother" and inevitably forces more careful analysis and far-reaching conclusions.

In recent years, the number of citizens registered in the Unified Identification and Authentication System (ESIA) has significantly increased in Russia. At the same time, unfortunately, the leakage of personal data of Russians has become more frequent, which fraudsters and other attackers use for criminal purposes.

Whenever it comes to high digital technologies, about their capabilities, ordinary Russians have thoughts about hackers who hack e-mail, making social networks not only business correspondence and trade secrets, but also the personal lives of citizens. They are capable, according to the US State Department, of interfering in the presidential elections, causing not only major damage to companies. It is no coincidence that the political elite of Russia on the eve of the elections to the State Duma of the Russian Federation expresses concern about the "Smart Voting", which was introduced and successfully applied by opposition politician Alexei Navalny during the elections of deputies to the Moscow City Duma and in a number of other regional legislative assemblies.

Can a hacker stop city infrastructure in the future? In 2015, Caesar Cerrudo of IOActive Labs conducted an ambitious experiment to show how smart cities are vulnerable to hackers. Cerrudo scanned the sensors used to control the movement. He found that their level of protection was so low that they could be manipulated, as a result of which the city could face large transport problems, as a result of which even fatal accidents could occur, and the operation of ambulances, firefighters or police would be difficult (Legal social network 9111, 2019). Sensys Networks, which maintains these sensors, reacted to Cerrudo's claims and accused him of exaggeration, but there was enough information about such a potential hazard for the authorities in Washington to decide to check the safety of the traffic management system. It is good that this vulnerability was discovered by a person who was trying to help. If an intruder were in his place, how could he use this information? In the future, such issues will more and more often have to be addressed by the authorities and state administrations, as well as by security experts. A smart city with a high level of connectivity increases the likelihood that someone could manipulate an entire infrastructure in the event that the proper level of security is not provided.

Digitalization of financial services not only made it easier for Russians to access their money in banks, but also represents a certain field of criminal activity for fraudsters. This conclusion is illustrated by the following graph (CBR, 2019).

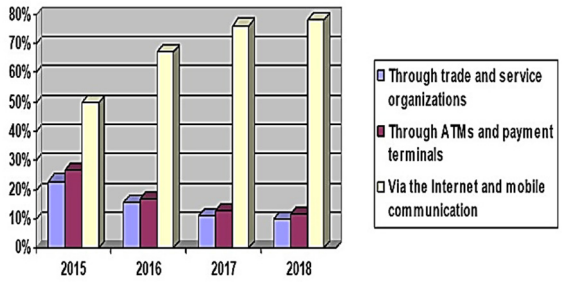

Figure 1: Unauthorized transactions using payment cards.

The above risks associated with the loss of money of the population due to the criminal activities of fraudsters using digital technologies are aggravated by the low level of "anxiety" of Russian consumers of banking services. Thus, according to opinion polls, 34 % of Russians in 2019 believe that there are no risks when using digital financial services. This conclusion is illustrated by the following diagram (Institute of National Projects, 2020).

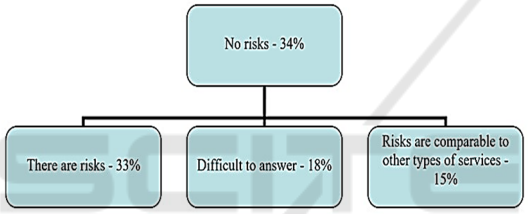

Figure 2: Public perception of the risks of using digital financial services.

It follows from the graph that the greatest risks and loss of money in 2015-2018 occurred due to unauthorized financial transactions that were carried out via the Internet and mobile devices. Thus, the digitalization of financial services not only made it easier for Russians to access their money in banks, but also represents a certain field of criminal activity for fraudsters. In this regard, banks need to decide how to reduce the risks associated with the digitalization of their financial services.

It is quite possible that behind the personification of "smart cities" with universal computerization and the power of IT technologies, there are quite prosaic interests of developers of relevant technologies and equipment such as HP, CISCO, IBM, promising to solve all the problems of modern cities with their help. While a lot has been said about predicting the dangers of smart homes, it is also important to assess the positive and negative aspects of smart cities, especially focusing on the problems of their safety.

Smart city apps are already being used to improve people's safety. The "city video surveillance system" has reduced the number of car thefts in the city by 80 % since its introduction (Legal social network 9111, 2019).

Of course, facial recognition can make the world a lot safer. There is one caveat, though. What opportunities do we want to transfer into the hands of the authorities? There are a number of nuances here. There are political parties that want to tackle online privacy, but many of them see encryption as a tool that is more necessary for criminals than to make people more secure against them. Is it worth sacrificing the online privacy of millions of ordinary people in order to be able to track the online activity of criminals and terrorists? This question is very difficult to answer. There are big risks here. Who exactly will have access to the huge volume of digital footprints of ordinary people with their daily lives that will be generated in the future? How will they use this data?

Billions of dollars are invested in smart city projects and can distract from other important issues worth pondering. For example, Indian Prime Minister Narendra Modi allocated $ 18 billion to connect 250 thousand villages to the Internet, although they do not even have clean drinking water and stable electricity supply (Gazeta.ru, 2015). The Ministry of Construction of Russia has developed the Smart City standard, covering 180 Russian cities. The project is estimated at 13 billion rubles (Zen.Yandex, 2019). This case is similar to India: in Russia more than a third of the regions still do not have gas supply, and in some places there is no electricity either. The reason is trivial - there is no money (MKRU, 2017).

Europe needs to invest 300 billion euros in its telecommunications infrastructure by 2025 if it wants to deploy a 5G network to accelerate economic growth and harness the potential of the technology. Such an assessment is contained in a study conducted by the consulting firm BCG (IXBT.com, 2021). Are there big risks? Governments of countries and public organizations should carefully analyze everything in order to understand what these technologies will bring more: benefit or harm.

4 SUMMARY

The study allows us to draw the following conclusions.

The study showed that in the presence of a number of positive digital transformations, such as openness, accessibility, transparency, convenience of functioning of the entire system of digitalization of public administration ", it is especially important for

the authorities and citizens to prevent the realization of the prospect of turning civil society into an automated community controlled by some powerful subject. This problem can be solved by strengthening and developing democratic institutions and tools for their functioning, and above all, if there is effective civic control and a high level of civic culture in society. In this case, citizens will be able to influence the system of digital management of social processes, and digital transformation will be carried out in their interests.

Over the 30 years of its existence, the smart city has turned from a constituent element of various discourses on management, technology, marketing, business, environmental protection into an independent discourse. This speaks of the need of the modern world for a "smart" organization of urban space in a constantly changing environment. At the moment, there are many questions in the conversation about “smart cities”. They relate to social, ethical or moral values. At the same time, today the scientific discourse about the smart city as a high-tech cities of the future is in the paradigm of "sustainable development", which includes the principles of the socio-cultural approach. This shows that the phenomenon is a socio-technical object. In an era of rapid technological development, the scientific community has seriously thought about the consequences of technology implementation. There is a rethinking of values, the role of technology in human life, ways of further development of mankind. All this forms the challenges that the “smart city” as a socio-technical phenomenon must cope with in order to prove its relevance and viability in the modern scientific paradigm.

It is also necessary to complete the creation of a regulatory framework for digital governance. For example, to clearly define the legal significance of digital documents and references in circulation that can replace paper media. The procedure for processing and executing citizens' applications on the website of public services needs further improvement, since responses to appeals are often delayed.

Digital democracy, which develops with the expansion of the activities of the "digital government", is quite vulnerable to outside influence in order to obtain information illegally. This danger arises from the lack of sufficient data protection. How cybersecurity will be ensured, which is mentioned, for example, in the plans of the Moscow authorities, is not yet clear. Digital transformation presupposes the formation of a complex digital control system that needs a high level of technological stability, which guarantees against frequent failures, user-friendly requirements for access to electronic services, which, in general, does not exist in Russia yet.

Digital transformation will be developed and used by people. This means that the state today is obliged to change its attitude to the problems of the formation, development and use of human capital. To pursue a well-thought-out policy in relation to this key factor in the socio-economic development of regions and the country as a whole, so that in the near future, if not catch up, then as close as possible to developed countries, where the share of human capital in the production of high-tech products reaches 70 %, while in backward Russia - only 14 %.

Scientists from Moscow State University (Leontyeva, 2021; Lyublinsky, 2020, Chaldaeva, 2020; Klimashevskaya, 2020). MADI (Moiseev, 2019), other Russian universities offer ways to improve the human capital of the regions and the country as a whole. The main thing now is that public authorities and administrations not only listen to their competent opinion, but also implement their scientifically grounded recommendations, then the risks associated with the digital transformation of management, as well as the economy and social sphere will be minimal.

ACKNOWLEDGEMENTS

The reported study was funded by RFBR, project number 19-29-07024/20

REFERENCES

"Smart city" will catch up with everyone, https://zen.yandex.ru.

«Umnyy gorod» 2019: spaseniye ili novoye moshenniches tvo? https://www.9111. ru.

According 2019 to the Central Bank of Russia, http://www.cbr.ru.

Alcaide, L. M., Rodriguez, B., 2018. *International E-Government Development Policy, Implementation and Best Practice.* Palgrave Macmillan. London. p. 320.

Asia leads the way 2017: the pros and cons of future smart cities, https://www.securitylab.ru.

Brown, A. J., Fishenden, M., Thompson, 2014. *Digitizing Government: Understanding and Implementing New Digital Business Models*. Palgrave Macmillan. London. p. 248.

Chaldaeva, L. A., Kilyachkov, A. A., Yakorev, A. A., 2020. On the issue of the formation of economic and organizational functions of public administration in the virtual space of Russia. *In Power.* 28 (2). pp. 63-73.

Davydenko, T. A., 2013. Human resources as an object of management in the "new" economy. *In Social and humanitarian knowledge*. 8. pp. 56-63.

Delcambre, L., Giuliano, G., 2005. Digital Government Research in Academia. *In Computer*. 38(12**)**. pp. 33-39.

Digital Literacy of Russians Research (2020), https://nafi. ru.

Europe 2021 needs € 300 billion to deploy 5G networks, https://www. ixbt.com.

Financial literacy 2020 in the context of digitalization: main risks and their management. Institute of National Projects. Moscow. p. 8.

FOM 2020: 22% of Russians have never used the Internet in their lives, https://www.newsru.com.

In India 2015 250,000 villages will have access to the Internet, https://www.gazeta.ru.

Klimashevskaya, O. V., 2020. Digital modernization of the Russian state and society: advantages, challenges and risks*. In Power*. 28(1). pp. 92-96.

Kochetkov, A. P., 2020. The Role of Digital Government in Improving the Effectiveness of Interaction between Government and Civil Society in Modern Russia. *In Politbook.* 3. pp. 18-32.

Leontyeva, L. S., Kudina, M. V., Voronov, A. S., Sergeev, S. S., 2021. Formation of national digital sovereignty in the context of differentiation of spatial development. *In Public Administration: Electronic Bulletin of Moscow State University M V Lomonosov.* 84. pp. 277-299.

Lovelock, P., Ure, J., 2013. *E-Government In China. The telecommunications Research Project.* University of Hong Kong.

Lyublinsky, V. V., 2020. Democracy and social policy in a digital network society. The reality of the present and the image of the future. *In Power.* 28(5).pp. 78-85.

Moiseev, V. V., Karelina, M. Yu., Komarova, O. A., 2019. Higher Education as a Factor in the Development of the Knowledge Economy in Russia. *In Advances in Social Science Education and Humanities Research.* 322. pp. 7-13.

Moiseev, V. V., Sudorgin, O. A., Karelina, M. Yu., Karelina, E. A., 2018. Social policy: yesterday and today. *In European Proceedings of Social & Behavioural Sciences EpSBS*. 50. pp. 817-830.

Novek, B. S., 2016. *Smart Citizens - Smart State: Expert Technologies and the Future of Public Administration*. Olymp-Business. p. 512.

Rudychev, A. A., Kazhanova, E. Yu., 2016. Evolution of human resource management objects. *In Bulletin of BSTU named after V G Shukhov.* 1(7). pp. 193-198.

Russia 2017 without gas: why a third of the country is shamefully not provided with it, https://www.mk.ru.

The Ministry of Defense 2021 announced a new type of US war against Russia, https://www.rbc.ru.

West, D. M., 2005. *Digital Government: Technology and Public Sector Performance.* NJ: Princeton University Press*)*. Princeton. p. 2.