Remote electronic voting in elections in Russia: State, problems, prospects

E. N. Bosova[1], *A. A. Chechulina*[2]

[1] Ufa University of Science and Technology,
32, ul. Zaki Validi, Ufa, 450076, Russian Federation
[2] Moscow University for the Humanities,
5, ul. Yunosti, Moscow, 111395, Russian Federation

For citation: Bosova, Elena N., Alla A. Chechulina. 2024. "Remote electronic voting in elections in Russia: State, problems, prospects". *Vestnik of Saint Petersburg University. Law* 3: 684–691. https://doi.org/10.21638/spbu14.2024.309

The paper examines the Russian experience of introducing remote electronic voting into the electoral process. By referring to the experience of other countries, we highlight the positive and negative aspects of remote electronic voting. The interest of states therein is due to the capability of combating the electorate absenteeism at polling stations for voting. Along with that, the results of surveying Russians on the use of remote electronic voting in elections show that some voters do not trust the outcomes of such voting for fear of fraud. We accumulated preferential provisions that constitute the interest of states in remote electronic voting. Blockchain technologies used in electronic voting are diverse and affect the public's attitude to the voting results in different ways, many electoral process participants do not understand the technical component of the electronic program. Russia uses a closed blockchain, therefore only the electoral process participants having a special key can view the data. It turned out that blockchain-based voting does not solve fundamental security problems, but on the contrary is technically more vulnerable than traditional paper ballot voting or postal voting. In Russia, legal regulation relates more to the technical aspects of organizing and implementing remote electronic voting in elections, but does not solve all the problems, leaving many gaps for the guarantees of citizens' electoral rights. Currently, the optimal model will be the combination of both traditional (paper ballot) and remote voting forms in order to reduce the risks of the latter, i. e. to apply a hybrid voting format in elections. Russian electoral legislation needs to be adapted to the hybrid format of elections with a paper ballot and an electronic ballot, providing voting rights of citizens and remote electronic voting.

Keywords: blockchain, ballot, elections, voting, remote voting, legislation, voters, secret ballot, electoral fraud, electronic voting.

1. Introduction

Economic and financial processes, as well as effective management of separate society's life aspects are no longer possible without electronic means in the modern world. In recent years, remote technologies have been increasingly gaining people's attention, and the pandemic undoubtedly contributes to this. Remote work has become a convenient and conscious choice of labor activity for many, and remote political process is unlikely to surprise anyone, although, we believe, it is still at the initial stage of populization among voters. Russia already has, although still limited, experience in organizing and implementing remote electronic voting, so far as part of regional and municipal elections. Government agencies

© St. Petersburg State University, 2024

are working in this field and, quite soon, federal level elections may be held in a remote format. Russia does not want to lag behind democratic countries that have been long using remote technologies for voting. Estonia has succeeded the most (Bosova, Reut 2019, 58).

Scientists from different countries are actively studying remote electronic voting. It is indeed interesting from a scientific and practical standpoint. Many are interested in the blockchain technology electronic system underlying the remote electronic voting process. With the electronic system features, scientists can realistically assess the risks affecting the election result, transparency and secrecy of voting, as well as other aspects.

Scientists analyze organizational aspects of remote electronic voting and reliability of the results thereof.

2. Basic research

2.1. Topic exploration degree

The topic of remote voting in elections is of great research interest. Scientific papers consider various aspects of remote electronic voting in elections, but most of the research is focused on the safety and risks of remote electronic voting.

In her paper, Melanie Volkamer studies electronic voting in general in order to understand its essence and determine its possible implementations. In particular, she conducted a comparative analysis of paper ballot voting and electronic voting, revealed the essence of remote electronic voting (including possible implementations of voter authentication, secrecy of voting and client-side voting) (Volkamer 2009). In his research, Burns Marlow presented expanded information about electronic voting systems (Marlow 2017).

The paper of Sunoo Park, Michael Specter, Heha Narula, Ronald L. Rivest analyzes and systematizes previous studies of online and electronic voting security risks and shows that these risks persist in both blockchain-based voting systems and can cause additional problems for voting systems in blockchains. They offer questions for a critical assessment of the security risks in new voting system proposals (Sinoo et al. 2020, 1).

Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed offer a blockchain-based system that ensures security, confidentiality and integrity. In their opinion, this system ensures voter's anonymity by storing information about the voter in the form of a blockchain hash (Tasmia Alvi et al. 2022). Nicholas Connolly considers security threats that can affect and compromise electronic voting system (Connolly 2022).

Chima Paul emphasizes that remote electronic voting system expands digital inequality. This means that electronic voting will favor only well-educated and wealthy people to the detriment of the destitutes in society. At the same time, he believes that the above Achilles heel of the transition from manual to electronic voting system is indirect and can be overcome over time by increasing voter awareness (Paul 2022).

This paper aims at studying the positive and negative aspects of remote electronic voting in terms of ensuring a democratic electoral process, as well as at analyzing the risks associated with remote technologies in elections, determining the prospects for the development of remote voting in elections to public authorities and local governments in Russia.

Research methods:

— the authors use sociological method to study the public opinion on the use of remote electronic voting in elections. The authors applied data from a survey of Rus-

sian citizens published by the Russian Public Opinion Research Center (VTsIOM) and the Center for Political Conjuncture in 2020[1]. Based on them, the paper concludes that although Russians are generally sympathetic to remote electronic voting, they still admit fraud with such voting method;

— the authors used comparative method to characterize the positive and negative aspects of remote electronic voting, as well as to assess possible risks associated with remote electronic voting and the development of the positive or negative public attitude to remote technologies in elections.

The authors identified the following positive aspects:

— blockchain technology-based electronic voting enables registering the elector's vote, excluding its falsification;

— increased voter turnout; the state can effectively fight absenteeism;

— economic efficiency;

— transparency and accountability of the voting process.

The authors believe that these advantages form a positive attitude towards the use of remote electronic voting in democratic states, including in Russia, and consider it a promising direction for the development of electronic voting technologies for citizens in elections and referendums.

The authors consider the negative aspects of using remote electronic voting based on the electoral practice of remote electronic voting in Russia for the regional parliament in 2019, in the Moscow City Duma, as well as based on a report by specialists from the Massachusetts University of Technology (Sinoo et al. 2020), where they categorically reject blockchain-based voting as a solution to election problems.

The negative aspects of remote electronic voting can be characterized as follows:

— possible control over the will expression of voters on the part of the administration;

— the principle of voluntary voting, the absence of coercion to vote cannot be traced;

— no real control over the voting results on the part of the members of the commissions and observers;

— participation in Internet voting which does not exclude hacker attacks on the network;

— digital inequality, etc.

Electoral practice in the 2019 regional elections in Russia has revealed the risks of remote electronic voting associated with technical shortcomings of the system and the use of a closed blockchain. Many negative reviews have appeared from politicians and experts. The reason for the ambiguous reaction was provoked by the fact that voters, as well as politicians, experts, observers, are not sufficiently aware of the technical subtleties of blockchain technology and diversity thereof. Blockchain programs can be open and closed, not everyone has access to transaction data. So, the elections to the Moscow City Duma in Russia in 2019 involved using a closed blockchain and a special key to access the system. The political parties did not receive that key, therefore they could not verify the data and received this system that ensured transparency of the voting results with incredulity.

[1] "Russian Public Opinion Research Center (VTsIOM) and the Center for Political Conjuncture present research data on the attitude of Russians to electronic voting in the context of testing this format for voting on amendments to the Constitution of the Russian Federation". *VTsIOM Novosti.* July 21, 2020. Accessed August 6, 2024. https://wciom.ru/analytical-reports/analiticheskii-doklad/pionery-internet-vyborov. (In Russian)

Therefore, states considering the prospects of remote electronic voting should pay attention to educating civil society about the technical features of voting transparency and obtaining election results using an electronic program.

The research of the legislation on elections regulating remote electronic voting involved the legal analysis method. It is noted that a full-fledged legislative framework for remote electronic voting has not yet been developed in Russia. Today, legal regulation relates more to the technical aspects of organizing and implementing remote electronic voting in elections, but does not solve all the problems, leaving many gaps for the guarantees of citizens' electoral rights.

2.2. Assessment of the positive and negative aspects of using remote electronic voting in elections

At first glance, remote electronic voting in elections has a positive effect due to the attractiveness to voters both for its technical novelty and encouraging interest in the exercise of the right to vote, since you can vote without visiting the polling station. In order to increase the percentage of voters in elections, states are striving to develop remote technologies. This is determined by the social and political development of each state, technical resources of state and municipal administration, the Internet availability for the population, and more. Of course, the state can contemplate the introduction of remote electronic voting only when most of the voters (presumably $^2/_3$) have an Internet connection, otherwise, investments in this remote process are unlikely to be justified.

By using remote electronic voting in elections, state authorities hope to reduce absenteeism of voters, since they may not visit the polling station and vote using either a computer or gadgets. Perhaps an innovative way of voting will be interesting for young people and attract their attention to participate in elections. It is noteworthy that in countries with high voter turnout, the interest of the state and the public in remote electronic voting is low (mainly the Nordic countries). In countries with low voter turnout (Great Britain) or frequent elections (Switzerland), as well as a complex system of counting votes (Belgium and the Netherlands), interest in remote electronic voting is high (Antonov 2011, 47).

But we should also take note that voters ignore voting in many ways not just because of their laziness or lack of time, but because they do not trust the authorities, believing that the election results are always falsified. We believe that the introduction of electronic means into the electoral process is promising both in terms of organizing the voting to be a little more convenient, and because it is necessary to ensure more transparent electoral process for public control. Falsifications, electoral corruption and other negative aspects of the electoral process are increasingly forcing society to distrust the election results. Therefore, countries having problems with the legitimacy of elections show great interest in the introduction of electronic voting, and vice versa. For example, in Sweden, voters trust the elections, their legitimacy in the country is very high, so experts fear that electronic technologies may break the established traditional electoral system (Antonov 2011, 50).

Experts pin a lot of hopes for solving these and other electoral problems in national elections on blockchain technologies that have already been successfully used both in the financial sector and also tested by countries in remote electronic voting in elections and referendums.

The state's interest in remote electronic voting is due to a number of its advantages, which can be described as follows:

— blockchain technology-based electronic voting enables registering the elector's vote, excluding its falsification;

— increased voter turnout; the state can effectively fight absenteeism;

— economic efficiency;

— transparency and accountability of the voting process.

Due to these advantages, a number of countries, including Russia, support the development of remote electronic voting. It is promising for the development of electronic voting technologies for citizens in elections and referendums. In general, following the example of countries such as Estonia, many states are trying to introduce the process of remote electronic voting in elections in their countries as the most promising (Volkamer 2009).

Public opinion polls of Russian citizens confirm the positive aspects of remote electronic voting[2]. Most of all, citizens are attracted by the mobility of electronic voting — 28 % of Russians surveyed are "for"; 50 % of Russians surveyed approved remote voting via the Internet; more than 20 % of Russians surveyed expressed concern about possible falsifications with this method of voting. It is understandable due to the prevailing negative opinion about possible manipulations with the results of voting in elections.

In 2021, the Central Election Commission of the Russian Federation organized an experimental voting of national elections in a test mode. The main task was to reach as many voters of the federal territory as possible. This shows Russia's interest in remote electronic voting in elections to the Russian parliament and in presidential elections.

In contrast to the positive view of remote electronic voting, there is also a negative one. The fact is that voters, political parties, observers may not understand the computer voting program, which is why they experience a technical and psychological barrier. In Russia, remote electronic voting has not yet been used in national elections, while it has been tested in local and regional elections: on March 1, 2009 — in the additional elections of the district Duma of Volgograd Region in Uryupinsk District; in 2019 — in the regional parliament to the Moscow City Duma; in 2022, remote electronic voting was implemented in seven regions on the Federal Remote Electronic Voting Platform (DEG) and in one region (Moscow) — on a regional DEG platform. Remote electronic voting used in the 2019 regional elections, due to the technical shortcomings of the system and the closed blockchain, did not allow the public to appreciate this system. Many negative reviews have appeared on the Internet from politicians and experts. The reason for the ambiguous reaction was provoked by the fact that voters, as well as politicians, experts, observers, are not sufficiently aware of the technical subtleties of blockchain technology and diversity thereof. Ignorance has given rise to many fears and rumors in the public and political environment.

The reason for the concerns is technical imperfection of the remote form of electronic voting, which has many negative aspects. Specialists of the Massachusetts Institute of Technology (Sinoo et al. 2020) categorically reject blockchain-based voting as a solution to election problems. They came to the conclusion that online voting in elections via blockchain creates more problems than it solves them. Among the negative aspects: the system vulnerability to unauthorized attacks, i. e. lack of cybersecurity, where its enhance-

[2] "Russian Public Opinion Research Center (VTsIOM) and the Center for Political Conjuncture present research data on the attitude of Russians to electronic voting in the context of testing this format for voting on amendments to the Constitution of the Russian Federation". *VTsIOM Novosti*. July 21, 2020. Accessed August 6, 2024. https://wciom.ru/analytical-reports/analiticheskii-doklad/pionery-internet-vyborov. (In Russian)

ment is associated with high costs; the system does not ensure the secrecy of voting; and other technical issues that do ensure complete confidence in the blockchain-based voting results. Experts conclude that the use of blockchain in remote electronic voting does not solve fundamental security problems, but on the contrary, it is more vulnerable than traditional paper ballot voting or postal voting.

The negative aspects of remote electronic voting can be characterized as follows:

— possible control over the will expression of voters on the part of the administration;

— the principle of voluntary voting, the absence of coercion to vote cannot be traced;

— no real control over the voting results on the part of the members of the commissions and observers;

— participation in Internet voting which does not exclude hacker attacks on the network, etc.

According to Chima Paul, the digital inequality of citizens is also the negative point (Paul 2022).

2.3. Technical support of remote electronic voting and voting security

Remote electronic voting involves blockchain technologies. The principle of blockchain operation is well described by a number of specialists (Marlow 2017), and details of this program are posted on the official website of the Central Election Commission of the Russian Federation. Often one of the positive aspects in the use of blockchain in voting is considered the capability of this technology to increase the confidence of citizens in the election results (Pollock 2018).

The blockchain stores all user entries, this confirms its transparency, if there are claims of violations, one can always check the voting results, which improves the security of elections (Lielacher 2018). Due to encryption and decentralization, the blockchain transaction database is incorruptible, and each entry is easy to verify (Liebkind 2020).

But, due to the variety of blockchain programs, they can be open and closed, not everyone has access to transaction data. So, the elections to the Moscow City Duma in Russia in 2019 involved using a closed blockchain and a special key to access the system. The political parties did not receive that key, therefore they could not verify the data and received this system that ensured transparency of the voting results with incredulity.

The situation with the DEG decryption key changed in September 2022, when parliamentary elections were held in a number of regions of Russia (from September 9 to 11 in Kaliningrad, Kursk, Novgorod, Pskov, Yaroslavl, Kaluga and Tomsk Regions, the federal city of Moscow). On the eve of the voting on September 8, 2022 in Moscow at a meeting of the Central Election Commission (CEC) of the Russian Federation, the decryption key of online voting was divided into ten parts. Then they were transferred to external media and handed over to the keepers. This year they are: The CEC of Russia, five parliamentary parties, the Civic Chamber of Russia, the Civic Chamber of the Kaliningrad Region, the Civic Chamber of the Tomsk Region and the Territorial Election Commission (TEC) for the DEG. After the voting completion on September 11, all parts of the key were collected again for summing up[3].

[3] "The Central Election Commission of Russia held a ceremony to share the decryption key for the DEG". *Tsentral'naia izbiratel'naia komissiia RF*. Accessed August 6, 2024. http://www.cikrf.ru/news/cec/52022. (In Russian)

Therefore, states considering the prospects of remote electronic voting should pay attention to educating civil society about the technical features of voting transparency and obtaining election results using an electronic program.

2.4. Legal regulation of remote electronic voting

The fact is that a full-fledged legislative framework for remote electronic voting has not yet been developed in Russia, although there are already certain advances in this field. In 2020, the Federal Law of June 12, 2002 "On the Basic Guarantees of Electoral Rights and the Right of Citizens of the Russian Federation to Participate in a Referendum"[4] is supplemented by the concept of "Remote Electronic Voting" (clause 62.1 of Art. 1). In 2022, this law was supplemented by Art. 64.1, which establishes the possibility of using remote electronic voting by decision of the relevant election commission, referendum commission during elections, referendums. Similar provisions are contained in federal laws regulating the election of the head of state and deputies of the Federal Parliament (clause 17 of Art. 69 of the Federal Law of January 10, 2003 "On the Election of the President of the Russian Federation", part 17 of Art. 81 of the Federal Law of February 22, 2014 "On the Election of Deputies of the State Duma of the Federal Assembly of the Russian Federation"). The procedure for organizing remote electronic voting in elections is regulated by by-laws: Resolution of the CEC of Russia of June 8, 2022 no. 86/716-8 "On the Procedure for Remote Electronic Voting Using Federal State Information Systems", Resolution of the CEC of Russia of June 8, 2022 no. 86/715-8 "On the Requirements for Remote Electronic Voting".

Today, legal regulation relates more to the technical aspects of organizing and implementing remote electronic voting in elections, but does not solve all the problems, leaving many gaps for the guarantees of citizens' electoral rights (Chechulina 2020). Established in the Constitution of the Russian Federation and federal legislation, the principle of secret voting with the participation of citizens in remote electronic voting is not guaranteed, since the voting procedure establishes that the voter must be a user of the federal state information system "Unified Portal of State and Municipal Services (Functions)" with a valid verified user account of this system. Thus, the will of the voters can be revealed if desired, while when filling out a paper ballot, the voter is provided with a booth for secret voting, where the presence of other persons is excluded. Therefore, the will of the voter is inaccessible to anyone except him-/herself (Bosova 2023). In addition, voting involves using the Internet and unauthorized intrusion into the system is possible. The grounds for appealing the voting and election results are also unclear. They are not established in the law when using remote electronic voting, although the conditions of electronic voting differ from that of paper ballot voting, therefore the grounds of appeal need to be expanded.

3. Conclusions

Remote electronic voting has both advantages over the traditional paper ballot voting, as well as disadvantages that do not fully ensure the security and secrecy of voting. According to the authors of this paper, security and protection against fraud are the main

[4] Hereinafter all references to Russian regulations are given according to the data from the "KonsultantPlus" system. Accessed August 6, 2024. http://www.consultant.ru. (In Russian)

issues that must be solved when implementing remote electronic voting. Currently, the optimal model will be the combination of both traditional (paper ballot) and remote voting forms in order to reduce the risks of the latter, i. e. to apply a hybrid voting format in elections.

Russian electoral legislation needs to be adapted to the hybrid format of elections with a paper ballot and an electronic ballot, providing voting rights of citizens in remote electronic voting.

References

Antonov, Yaroslav V. 2011. "International experience of electronic voting". *Sbornik konkursnykh rabot v oblasti izbiratel'nogo prava i izbiratel'nogo protsessa vypolnennykh studentami, aspirantami v 2010/2011 uchebnom godu*, 43–60. Moscow, RTsOIT Publ. (In Russian)

Bosova, Elena N. 2023. "Secret expression of the will of voters: Traditional and remote". *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta* 1 (17): 27–33. https://doi.org/10.33184/vest-law-bsu-2023.17.3 (In Russian)

Bosova, Elena N., Dmitrij A. Reut. 2019. "Remote electronic voting: Search for legislative formalization". *Pravoprimenenie* 3: 53–62. https://doi.org/10.24147/2542-1514.2019.3(3).53-62 (In Russian)

Chechulina, Alla A. 2020. "The concept of judicial law: Russian context". *Amazonia Investiga* 9 (25): 223–229.

Connolly, Nicholas. 2022. *Issues with Electronic Voting*. Accessed August 6, 2024. https://www.researchgate.net/publication/252859151_Issues_with_Electronic_Voting.

Liebkind, Joe. 2020. "How blockchain technology can prevent voter fraud". *Investopedia.* Accessed August 6, 2024. https://www.investopedia.com/news/how-blockchain-technology-can-prevent-voter-fraud.

Lielacher, Alex. 2018. "How blockchain could secure elections". *CBINSIGHTS.* Accessed August 6, 2024. https://www.cbinsights.com/research/report/blockchain-election-security.

Marlow, Burns. 2017. "Fundamental, unequivocal, yet unreliable: The interplay of voting, electronic voting systems, and trade secrets in today's interconnected world". *Journal of Intellectual Property Law* 24 (2): 381–415. Accessed August 6, 2024. https://digitalcommons.law.uga.edu/jipl/vol24/iss2/7.

Paul, Chima. 2022. "Transiting from manual voting to electronic voting system for enduring democratic governance in Nigeria: The imperative for digital remedy". *Journal of Technology Innovations and Energy* 1 (1): 9–18. https://doi.org/10.56556/jtie.v1i1.131

Pollock, Darryn. 2018. "Blockchain for elections: Advantages, cases, challenges". *Cointelegraph.* Accessed August 6, 2024. https://cointelegraph.com/news/blockchain-for-elections-advantages-cases-challenges.

Sinoo, Park, Michael Specter, Neha Narula, Ronald L. Rivest. 2020. *Going from Bad to Worse: From Internet Voting to Blockchain Voting. Report by MIT Specialists. November 6, 2020 (DRAFT)*. Accessed August 6, 2024. https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf.

Tasmia Alvi, Syada, Nasir Uddin Mohammed, Islam Linta, Ahamed Sajib. 2022. "DVT chain: A blockchain-based decentralized mechanism to ensure the security of digital voting system". *Journal of King Saud University — Computer and Information Sciences* 34 (9): 6855–6871. https://doi.org/10.1016/j.jksuci.2022.06.014

Volkamer, Melanie. 2009. "Implementations of electronic voting". *Lecture Notes in Business Information Processing*, 30. Accessed August 6, 2024. https://www.researchgate.net/publication/251203082_Implementations_of_Electronic_Voting.

Received: February 15, 2023
Accepted: April 29, 2024

Authors' information:

Elena N. Bosova — PhD in Law, Associate Professor; https://orcid.org/0000-0003-4888-7424, bosova_elena@mail.ru
Alla A. Chechulina — PhD in Law, Professor; https://orcid.org/0000-0003-0303-1219, Cha11@yandex.ru