

SECTION 1. A CONSTITUTIONAL RIGHT

DOI: 10.46299/ISG.2024.MONO.LEGAL.3.1.1

1.1 Risks of e-voting in post-war Ukraine

After the end or lifting of martial law on the territory of Ukraine, the state will face an extremely difficult task - to hold post-war elections. What these elections will be like, taking into account all the problems of the electoral procedure both inside Ukraine and abroad, must be determined now.

Given that the regular parliamentary and presidential elections in Ukraine have not taken place (although they should not have), calls for online voting, for example, through Diia, are increasingly being heard in Ukrainian society. This seems to the public to be a simple and logical solution to the problems associated with the impossibility of holding elections in the traditional way during martial law or immediately after its completion.

Some Ukrainian scholars hold the same position, emphasizing that the digitalization of the procedure for holding elections and referendums in Ukraine is inevitable. And this applies not only to online voting, but also to voting with the use of technical means at polling stations and even the use of Blockchain systems. Moreover, the legislator has already enshrined provisions on electronic voting in the electoral and referendum legislation. However, such a decision may be unjustified, which is why this topic is relevant.

Given the above, the purpose of the study is to prove that the use of any type of electronic voting, including Internet voting, during elections and referendums in Ukraine cannot be considered an appropriate solution.

In order to achieve this goal, the following tasks were set:

- 1) to analyze the positions of domestic scholars and the public on the introduction of electronic voting in Ukraine;
- 2) to study the experience of foreign countries that have already used electronic voting;

3) to consider the views of foreign scholars, IT specialists, government officials, etc. on e-voting.

The research should result in legislative proposals aimed at preventing the use of e-voting in elections and referendums in Ukraine. Also, the result of the work can be considered a contribution to the formation of an idea about the inexpediency of introducing e-voting.

Electronic voting is a relatively broad term that includes both voting directly at polling stations using electronic devices and various kinds of equipment; and voting outside of polling stations using the Internet - Internet voting. In addition, it is worth mentioning the holding of elections using Blockchain technology. All these manifestations of electronic voting pose a significant threat to the electoral process in Ukraine, but domestic scholars, turning a blind eye to potential risks, often emphasize the advantages of e-voting. Let's start with them.

The use of remote Internet voting will provide «the possibility of voting regardless of the voter's location, which is a guarantee of observance of the right to vote for voters who are unable to come to the polling station on election day and vote with an absentee ballot. Therefore, we can talk about increasing the turnout at the elections...» [1]. Given the millions of Ukrainians who left the territory of Ukraine after February 24, 2024 and did not return, as well as the significant number of internally displaced persons who will not be physically able to vote at the polling stations to which they are assigned (especially in the context of those polling stations that were lost due to the occupation), the use of Internet voting can indeed facilitate the exercise of their active suffrage by voters. However, the following should be noted in this regard:

- 1) The mere possibility to vote remotely is not enough: it is necessary to create equal conditions for the exercise of active and passive voting rights for both Ukrainians living in Ukraine and those abroad. For example, the issue of political campaigning abroad remains unresolved; the same can be said for compliance with Ukrainian electoral legislation (even with online voting) and bringing those responsible to administrative or criminal liability. After all, the level of mutual understanding and cooperation between Ukraine and other states

can vary significantly in each case. And the difference may be especially noticeable in relation to the election process in Ukraine itself.

- 2) The issue of changing the polling station for internally displaced persons is resolved by submitting a voter's application for a temporary change of voting place without changing the voting address. And for voters who will be residing abroad at the time of the election, there is an opportunity to vote at a polling station abroad (the state must ensure the availability of premises, personnel and other aspects necessary for holding elections in the traditional form).
- 3) And finally, looking ahead a bit, let's look at the experience of foreign countries in using online voting: «There is no evidence that online voting in Estonia led to an increase in voter turnout. The analysis shows that the overall turnout did increase slightly after the introduction of online voting, but it cannot be said that this was due to online voting alone» [2].

As for increasing the turnout in general, in particular, by involving young people in the voting process through the introduction of Internet voting, it should be noted that such a solution will not yield significant results. It doesn't matter what technologies are involved in the electoral process: «simplification of the voting procedure alone cannot produce civic engagement among passive youth, which is the main problem» [3]. Instead, it is necessary to raise the level of political and civic awareness of the population in general, to make it clear that every vote is important and that the outcome of the election/referendum depends on the decision of citizens. It is important to restore voters' trust in both the authorities and the election procedure, which will result in an increase in voter turnout.

The advantages of introducing electronic voting in Ukraine also include potential economic benefits: «by reducing the cost of organizing elections» [4]; «when using electronic voting, it is possible to minimize the cost of holding elections» [1]. In addition, the advantage of e-elections is «environmental friendliness - by reducing the use of paper in elections» [4].

However, it is not possible to completely replace traditional elections with electronic ones, since not all voters have a stable Internet connection and the necessary

devices (smartphone, computer) to participate in online voting. Another problematic aspect is the overall level of digital literacy of the Ukrainian population, especially among the elderly. In view of the above, only a mixed form of elections can be considered, where certain electronic voting technologies are used in parallel with the traditional format of elections.

It follows that in case of introduction of electronic voting, the costs of holding elections will only increase, as there will be an additional need to purchase expensive equipment, transport it to each polling station, train election commission members (basic use of equipment, configuration skills, correcting errors in case of malfunction, etc. etc.), as well as the development of an online resource for Internet voting that is fully protected from external and internal cyber threats, which seems to be impossible in principle.

From an environmental point of view, the situation will not actually change: the mixed form of elections will require the same use of paper as usual, because it is not known how many voters will come to the polls in person and how many will decide to use online voting. Given the aforementioned low level of digital literacy among voters, it will not be possible to do without using paper at all, even if technical means are used at polling stations. After all, in our case, it is advisable to use only «information systems for optical scanning of ballots, which are a combination of traditional and electronic voting» [3], where the voter fills out a regular paper ballot and «throws» it into an electronic ballot box. Instead, as it becomes clear from the above, «information systems for direct recording of votes» [3], which do not require the use of paper, cannot be involved in the electoral process. In addition, it is worth noting that any technical means require the use of electricity, which also has a negative impact on the environment.

Turning to the disadvantages of electronic voting, it should be noted that neither Internet voting nor voting with the help of technical means that provide for automatic voter authentication ensure the secrecy of voting, as required by the provisions of the Constitution of Ukraine, the Electoral Code of Ukraine, the Code of Good Practice in Electoral Matters and other acts.

After all, electronic authentication will require a voter to provide proof of his or her identity by using an electronic signature, scanning a passport, fingerprints, etc. Only after such a procedure will the voter be able to cast his or her vote, but it is obvious that in this case, the secrecy of the vote is out of the question. For greater understanding, an analogy can be given: this method of voting is not much different from a hypothetical situation where a voter, before throwing a completed ballot into the ballot box, shows its contents to members of the election commission.

The problem with Internet voting is that the state cannot, in principle, ensure the secrecy of the vote for voters who will be located even outside Ukraine. As a result, it will be virtually impossible to prevent pressure on voters during the vote. However, some foreign countries have found a solution (only partial) to this problem. For example, in Estonia, in order to prevent pressure on voters, the duration of online voting is set at several days before the day of traditional elections. At the same time, the voter can change his or her decision an unlimited number of times, and the final vote in this case is considered to be the last vote or the one cast in the traditional form (after which remote voting is impossible). As the Supreme Court of Estonia has established: «The Court considers that the possibility to change the result of one's own electronic voting is necessary to guarantee freedom of elections and secrecy of voting» [2]. However, this approach opens up a wide field of possibilities for cyberattacks, primarily by the aggressor country, on online resources, equipment, and even private voter devices used during elections. It also does not eliminate the threat that, when using Internet voting, a voter can be observed by others (regardless of whether the voter knows about it) even when the voter is casting his or her vote.

The next disadvantages of electronic voting, which to some extent correlate with each other, are the threat of falsification of election results by the authorities and the impossibility of prosecution for election offenses. In terms of fraud, the following arguments are made in favor of electronic voting: «No one else will be able to use the ballots that voters did not use, and no one else will be able to put bookmarks in the ballot box, because there are neither ballot boxes nor ballots», «there will be no use of dead souls» [5]. However, despite the absence of these risks when using e-voting, the

possibility of fraud does not disappear. Moreover, the authorities get much wider opportunities to use the «administrative resource» to influence the election results, since it is impossible for independent observers to track the course of electronic voting. Here, the example of the Russian Federation comes to mind, where «pro-government» candidates were «added» votes through electronic voting.

As you know, «electronic voting protocols have a single controller who controls the entire voting process... however, this approach leads to erroneous elections due to the dishonesty of the central government (election commission), which is difficult to correct by existing methods» [6]. In other words, if electronic voting is used, it will be enough for the authorities to control the activities of the Central Election Commission to successfully falsify elections. Moreover, the absence of the so-called «paper trail» will make it impossible to verify the voting results in connection with any circumstances that may cast doubt on the validity of the final voting results. For example, a system failure due to a cyberattack.

Thus, when electronic voting is used, it becomes virtually impossible to prove the fact of violation of electoral legislation and further identify the perpetrators (especially abroad) and bring them to justice. It becomes obvious that electronic voting cannot be an effective way to solve the problem of illegal interference in the electoral process. With e-voting, falsification does not disappear, only its dimension changes: from «live» to digital.

As already mentioned, the introduction of electronic voting in elections and/or potential referendums in Ukraine will inevitably entail an unlimited number of attempts to interfere in the electoral process from the outside, through massive cyberattacks.

Such a threat exists primarily in the case of Internet voting (although it is also quite possible to hack into electronic technical means of recording/counting votes at polling stations or the databases themselves). And the main actor interested in this is, of course, the aggressor country, the Russian Federation. This was clear even before the outbreak of a full-scale war: «the biggest disadvantage of introducing an electronic election system in the realities of modern Ukraine, which is repelling hybrid aggression, is still

the possibility of cyberattacks on the system, especially from the aggressor country» [5].

Confirmation of this thesis does not even require in-depth research: Ukraine has already had experience in repelling cyberattacks initiated by the Russian Federation to disrupt the electoral process in our country. For example, on the eve of election day during the 2014 early presidential elections in Ukraine, Russian specialists gained access to the Central Election Commission's databases, in particular, to the Unified Information and Analytical System «Elections», where they deleted information from the relevant databases. «The CEC... managed to restore the system of establishing the election results just an hour before the opening of polling stations on election day» [7].

Of course, over the past 10 years, the electronic systems used in Ukraine's elections have been significantly modified in terms of cybersecurity. However, the introduction of electronic voting, which is new for Ukraine, will also provoke a new wave of cyberattacks aimed at discrediting or even changing the voting results. The current leadership of the Russian Federation is incredibly interested in this scenario of elections in Ukraine, as it refuses to recognize the «post-Maidan» government (considering the Revolution of Dignity a coup d'etat); and emphasizing that democratic elections are not held in Ukraine in principle. Russia will try to discredit the course of voting in our country in order to use it in the future to legitimize its armed aggression against Ukraine internationally.

In addition to the threat from Russia, there are other risks in the event of the introduction of online voting: «It is possible that the source of hacker threats may also be within the society where Internet voting takes place (insider attacks), or election officials may inadvertently allow outside interference in the voting process (trojan attacks)» [8].

As an example of foreign countries, we can cite the United States of America, South Africa, and Israel, where attempts to launch a cyberattack on information and communication technologies used in elections were also recorded [2]. The experience of Israel, which is also in a state of military conflict, is particularly relevant for Ukraine. Even in such a difficult situation, the state's leadership made a serious mistake when

developing the voting application: «In 2020, there was a large-scale leak of personal data of almost 6.5 million Israeli citizens. The source of the leak was the Elector voting app. Almost the entire voter register could be downloaded by anyone. And the reason was the usual negligence of the developers: the program code contained an API in the open form, which allowed to obtain a list of all users of the system with unencrypted passwords» [9]. There is no guarantee that Ukrainian IT specialists will not make a similar mistake and that Russia will not take advantage of it.

A good example is the events that accompanied the online voting in Switzerland in 2023. At that time, computer scientist Andreas Kuster was able to identify the weaknesses of the local electronic voting system on his own [10]. I would like to note that this was done by one person, but what about the entire headquarters, whose work is directly funded by the state with one goal - to prevent Ukraine from holding democratic elections?

Speaking about the experience of foreign countries in using electronic voting, it should be noted that at the beginning of the century, interest in the new technology began to grow rapidly, which translated into corresponding changes in the electoral process within countries. However, later, with the development of crime in the IT sphere, some states refused to use e-voting.

For example, the Netherlands returned to traditional elections in 2008, when it became apparent that it was impossible to comply with the principle of secrecy of the will using e-voting.

In Germany, the initiative to introduce Internet voting was stopped by the decision of the German Constitutional Court in 2009: «Internet voting is unconstitutional and violates the principle of publicity, as it requires that all stages of the election, including voting and counting, be subject to public scrutiny and do not require special knowledge» [11]. By the way, there is every reason to believe that the Constitutional Court of Ukraine would also have blocked the relevant law.

And for cybersecurity reasons, Norway (2014), Canada (2017), Switzerland (2019) (although in 2023 the country returned to e-voting, but, as demonstrated above, in vain), and France (2017) - only for voters abroad. Also, «in 2019, the Lithuanian

government abandoned the idea of introducing online voting in elections precisely because of the threat of cyberattacks» [1].

The experience of Switzerland and its persistent attempts to implement the I-voting technology, despite all the risks, is worth noting: Switzerland is a unique country that regularly holds referendums at the national level (several a year). This can tire citizens and, as a result, the turnout will decrease. Also, such frequent holding of referendums in the traditional format requires considerable financial costs, so, in fact, Switzerland has no choice but to find a truly reliable online voting system.

Estonia's practice is often cited as a successful example of full digitalization of elections. This is not surprising: Estonia has been practicing electronic voting, in particular via the Internet, since 2005 and is not going to abandon the technologization of the electoral process. However, Piret Ehin and Mihkel Solvak from the University of Tartu and Jan Willemson and Priit Vinkel, representing the Estonian technology company Cybernetica AS, wrote a joint research paper analyzing Estonia's experience in using Internet voting from 2005 to 2019 [12]. The experts came to the following conclusions:

1) «**Internet voting complicates election administration** instead of simplifying it. By deploying i-voting, governments take on a long-term obligation to develop technology, build legal frameworks, adjust election administration, and defend the system against attacks, criticism, and disinformation on both the domestic and the international arena» [12];

2) «the deployment of **Internet voting does not increase electoral participation...** Aggregate data from eleven Estonian elections shows that despite massive uptake of i-voting, rates of electoral participation have remained stable. This... suggests that Internet voting facilitates electoral participation for those who intended to vote anyway. It does not motivate non-voters to take part in elections» [12];

3) «final conclusion reiterates the **importance of trust** as a precondition for the adoption and use of new technologies. Our data showed that in Estonia, trust in Internet voting is the single most important predictor of casting an electronic ballot as opposed to a paper one» [12].

Thus, the use of electronic voting, even in foreign countries, creates certain problems and raises concerns among the public, scholars, experts, and authorities, especially the judiciary. In addition, the trust of Ukrainian society in the results of elections held electronically, in particular via the Internet, is unlikely to be conditionally sufficient. And it should not be.

Given the growing interest of the domestic scientific community in the use of Blockchain technology for elections, this initiative cannot be ignored [4], [13]. It should be noted at once that the author of the study is not an IT specialist and therefore will not provide a detailed description of the problems of using Blockchain from a technical point of view. Instead, it will be advisable to refer to the position of authoritative experts in the relevant field. Thus, in 2021, the Journal of Cybersecurity published an article titled «Going from bad to worse: from Internet voting to blockchain voting» [14].

In the article, the authors prove that there are security and other risks associated with any type of electronic voting. Thus, the arguments are presented regarding:

1. With the introduction of Blockchain technology, the electoral procedure becomes significantly more complicated. For example, in the event of a failure or cyberattack, it will be more difficult to restore the Blockchain voting system: «Because decentralized systems do not have a single point of control, changing the protocol, even for the sake of addressing vulnerabilities, requires coordination. This means it takes more time and effort to deploy security fixes in a decentralized system than in a centralized one, and blockchain systems can be vulnerable for longer periods of time than centralized counterparts» [14];

2. Describing the voting mechanism itself, which is used in the Blockchain for various purposes outside the electoral process, the authors note: «[now] users can bet on the outcomes of sporting events, market movements, weather, and more... **These kinds of processes do not fulfill the requirements for secure voting in elections** and are designed for a very different purpose with a different threat model» [14]. In other words, the authors emphasize that Blockchain technology cannot be used for elections,

despite the fact that various kinds of voting and polls are already being conducted today (here we should mention «Diia»). Different degrees of responsibility and threats.

3. The study concludes with three main conclusions:

- 1) «Electronic, online, and blockchain-based voting systems are more vulnerable to serious failures than available paper-ballot-based alternatives. Moreover, given the state of the art in computer security, they will continue to be so for the foreseeable future» [14];
- 2) «Blockchain technology does not solve the fundamental security problems suffered by all electronic voting systems. Moreover, blockchains may introduce new problems that nonblockchain-based voting systems would not suffer from» [14];
- 3) «Adding new technologies to [voting] systems may create new potential for attacks. Particular caution is appropriate in security-critical applications, especially where political pressures may favor an expedited approach [on the introduction of electronic voting]» [14].

Thus, lawyers and cybersecurity experts are unanimous on the issue of introducing new technologies into the election and/or referendum process. The decision of the Ukrainian legislator to introduce e-voting may be premature, or even fundamentally wrong, which will lead to irreparable consequences.

In view of the above, it is proposed to amend the Electoral Code of Ukraine, namely, to remove Article 18 «Use of Innovative Technologies in the Electoral Process» and other provisions of the Code that develop the provisions of Article 18 [15].

This decision seems logical, given the content of Article 18 of the Code, which provides for:

- 1) «voting at the polling station with the help of technical means and software (machine voting)» [15] - due to the impossibility of ensuring voter anonymity;
- 2) «counting of votes using technical means for electronic vote counting» [15] - due to the impossibility to verify the correctness of the count, to conduct a repeat vote count;

3) «drawing up protocols on vote counting, results and results of voting using the information-analytical system» [15] - the same as in paragraph «2)».

It is also proposed to exclude the provisions on electronic voting in the Law of Ukraine «On the All-Ukrainian Referendum», in particular, the law «on the use of innovative technologies for electronic (machine) voting» [16].

It may seem that electronic voting, especially Internet voting, is the key to solving the problems of post-war elections in Ukraine. However, the introduction of innovative technologies in the electoral process creates many risks and potential negative consequences. Any benefits from the introduction of e-voting cannot outweigh the parallel growing scale of threats.

It is also worth noting that citizen participation in elections and referendums is a form of direct democracy, where people express their position and shape the vector of further development of the state. Elections and referendums are not just another sociological survey that you can take part in in 30 seconds while lying on the couch.

The process of digitalization of public services that citizens face every day should not affect elections. After all, every national election and referendum is a significant and extremely responsible event that requires proper «support».