CEMI
CENTRE FOR MONITORING AND RESEARCH

# REVIEW OF TECHNOLOGY FOR CONDUCTING ELECTION ACTIVITIES IN MONTENEGRO

May 2021
Podgorica, Montenegro

# POLICY BRIEF

# REVIEW OF TECHNOLOGY FOR CONDUCTING ELECTION ACTIVITIES IN MONTENEGRO

CENTRE FOR MONITORING AND RESEARCH

Bulevar Josipa Broza 23 A, 81 000 Podgorica, Montenegro
Email: info@cemi.org.me
**www.cemi.org.me**

**Editor:**
Zlatko Vujovic

**Author:**
Vladimir Simonovic

**Circulation:**
100

British Embassy
Podgorica

**NOTE:** The opinions and views expressed in this policy brief represent the opinion of the authors and do not necessarily reflect the official views of the donors.

# INTRODUCTION

Bearing in mind that technology plays a major role in our daily lives, as well as an increasing role of technology in the election process, CeMI decided to review the current state of technology for conducting election activities, as well as the legislation that regulates the area relevant for the use of modern technical devices in elections.

Technology develops quicker than laws meant to regulate it. Therefore, minimising the problems that stem from the introduction of the process of modernisation of the electoral process requires a set of activities and measures, which, besides acquiring and testing the necessary technological equipment, involves changes and amendments to the existing legal documents that would ensure the safe use of new hardware and software solutions relevant for conducting of electoral activities.

The use of modern technology for conducting election activities in Montenegro is still in its infancy, which contributes to the security of the entire election process in terms of risks that accompany modern technical solutions. In Montenegro, for example, there is no electronic voting, and therefore no electronic vote counting. Therefore, the public trust in the procedure of vote counting is not an issue in Montenegro. The lack of trust in the electoral process revolves mostly around activities conducted during the pre-election period and around the irregularity of the voter register.

Montenegro will continue to upgrade its IT capacities, which constitutes upgrades to how the election administration bodies operate, and how the entire electoral process is conducted, from the IT perspective. However, the technological modernisation carries certain risks that require special attention, as technology can have a crucial impact on the conduct of fair elections.

This policy brief before you is one of the results of the project of civic monitoring of local election in Niksic 2021, and it represents a review of the technical solutions currently available to the election administration bodies for conducting election activities. Also, the brief presents the basic technical and legal deficiencies that need to be solved in order to improve and upgrade the safety of the election administration bodies and the electoral system.

# TECHNOLOGY FOR CONDUCTING OF ELECTORAL ACTIVITIES IN MONTENEGRO

Among the hardware and software solutions used to conduct election activities in a broader sense, we can list: devices for electronic voter identification, AFIS civilian system for deduplication of voter fingerprints, software for verifying signatures of support for the electoral lists, online service biraci.me service and online service potpisi.dik.co.me. In a strict sense, this includes only devices for electronic voter identification and software for verifying signatures of support for the electoral lists.

Electronic voter identification devices have been used in Montenegro since 2016. The use of these devices has modernized the voting process, but it has not significantly contributed to increasing the level of citizens' trust in the electoral process. Electronic voter identification devices are described in the Law on the Election of Councillors and MPs as a compact hardware and software unit composed of: 1) electronic reader of machine readable zone (MRZ) on ID card and passport; 2) computer into whose memory the extract from the concluded electoral register for a precisely designated polling station shall be uploaded, including the last photo of voter from the registers of ID cards or passports and 3) printer to print the confirmation of successful voter identification.[1]

These devices contain information about the polling station where they were activated, the date, time and excerpt from the voter register for that polling station and for the elections that are being held. Each device contains only the turnout statistics for the polling station where the device is located. By swiping the ID card or passport through the reader on the device, the data on the voter appear, if the voter is registered at that polling station.

Electronic voter identification devices are owned and controlled by the Ministry of the Interior, as the body in charge of maintaining the voter register. They are not connected to the Internet, nor is there a possibility to download the data stored in them. Also, the devices are not interconnected, and the data stored in these devices is deleted within 30 days from the date of publication of the final election results.[2]

On the one hand, the decentralisation of electronic identification devices and complete separation from other devices contributes to the security of voters' personal data, but on the other hand, this opens the possibility of multiple

[1] Article 68 of the Law on Election of Councillors and MPs, ("Official Gazette of Montenegro", no. 16/2000, 9/2001, 41/2002, 46/2002, 45/2004 – Constitutional Court [CC] decision, 48/2006, 56/2006 – CC decision and "Official Gazette of Montenegro", no. 46/2011, 14/2014, 47/2014 – CC decision, 12/2016 – CC decision, 60/2017 – CC decision, 10/2018 – CC decision and 109/2020 – CC decision)

[2] Ibid, paragraph 5

voting, in case one voter is registered at several polling stations. In addition, these devices completely depend on the external power supply, i.e., they do not have an internal power source, so in the event of a power outage at the polling station, the electronic voter identification device cannot function. This shortcoming can be eliminated only by purchasing new devices with an internal power supply system, i.e., modification of existing ones is not possible.

Another modern solution used in the Montenegrin system is the software for processing the election data, which the SEC received from the OSCE Mission to Montenegro in 2019. The total value of the software, two servers and accompanying hardware was 170,000 euros.[3]

The software donated by the OSCE to the SEC contains, among other things, a module for processing data on voter turnout and polling station results. The main function of this module is reflected in the creation of reports. Two people are responsible for the accuracy of the data – one person at the polling station and another in the Municipal Election Commission who checks the data obtained from the polling boards. The way that this part of the software works is as follows: the competent person at the polling station enters the data into the software, which cannot be changed after confirmation. After entering the data, an electronic record is created which is sent electronically for verification to the MEC. In case an error occurred during data entry, the responsible person in the MEC will delete that record and create a new one with corrections. The software also contains a functionality for exporting preliminary results to the SEC website.

The software operates through a VPN and has firewall protection. For the purpose of safety of the data, the VPN service is provided by the British company for data protection and information systems, Sophos.[4]

Although the SEC uses the services of a reputable company with extensive experience, it is not possible to assess the security of the software solution available to the SEC, that is, the possibility of an external attack that could potentially alter the voting results, or the possibility of disabling the system through a ransomware attack, DDoS attack etc., because the software has not yet been used in the elections, and security has not been checked by simulated attacks, the so-called breach and attack simulation (BAS).

According to our interlocutor from the SEC, the software has been tested and it works. However, the barrier to its application is the Law on Election of Councillors and MPs. According to the Law, the only electronic device whose use is allowed at the polling station is a device for electronic identification of voters, and members of the polling station committee are obliged to be present at the polling station all the time, which means that existing the polling station to send the results to the MEC would

[3] https://www.osce.org/me/mission-to-montenegro/411812
[4] https://www.sophos.com/en-us.aspx

constitute a violation of the law.

In order to fully enable the use of this software module, it is necessary to amend the Law on the Election of Councillors and MPs to provide for the possibility of an additional electronic device (computer or mobile phone) that would be used exclusively for this purpose and designate the person responsible for operating that device. In addition, it is necessary to provide a sufficient number of devices for each polling station, training for the use of the device as well and to ensure proper safety during its use.

Another important software module available to the State Election Commission is the module for verifying signatures for the support of electoral lists. This module, however, is not adequately designed. Namely, the manner of verifying the signatures is not in line with the needs of the State Election Commission, bearing in mind the legal obligation of the SEC to check whether the list of signatures within 48 hours of receiving the electoral list, and considering the possibility for submitters of electoral lists to submit signatures of support at any time until the deadline for submission of electoral lists and without prior notice. Considering that the software requires users to enter the name, surname and the ID number of the person who signed the list of support for the electoral list, as well as due to the lack of capacities of the State Election Commission to process a large amount of data in a short period of time, during the Parliamentary elections in 2020 the State Election Commission decided to use an application developed by the IT Office of the Parliament of Montenegro. Their software solution for verification of signatures requires only the entry of a unique ID number, which contributes to faster data processing. In addition, due to the lack of capacity for timely data processing, The State Election Commission has decided to entrust the data processing to persons employed in the Office of the Parliament of Montenegro, which the Agency for Personal Data Protection has assessed as illegal.[5]

It is important to point out that the State Election Commission has the source code of the software donated to them by the OSCE, so there is a possibility of subsequent modification of signature verification module to suit their needs. In that sense, the biggest barriers are the financial resources and capacities of the State Election Commission.

The State Election Commission does not currently have admirable technology with a satisfactory level of security for the daily work of other employees. The aforementioned software is used exclusively for elections and does not contain a module for office operations and archiving. The servers donated to the SEC together with the election data processing software are connected only to said software. The maintenance of the SEC website is currently entrusted to an external company.

Aside from the fact that the SEC does

[5] https://tinyurl.com/2ms7bh2n

not possess relevant software for office operations and archiving, there is currently no system of control and inventory of authorized devices and software that its employees use, nor an automated data backup system. SEC system administrator can access all computers on the network, but each employee takes care of the data protection on their device. All computers used by employees are password protected, but it is unknown how "strong" the passwords used by employees are, because the State Election Commission does not hold trainings for employees on digital hygiene and cyber security, so the level of digital literacy of the employees in the State Election Commission, which would ensure the level of awareness necessary for recognizing the importance of quality protection of computer systems is questionable.

In the coming period, the State Election Commission plans to establish an active directory on the third server at its disposal, along with software for office operations that all employees will be connected to, and active control of hardware and software, as well as automated update of software and data backup will be implemented. It is also planned that SEC website and e-mail server be migrated to this server, which will not be connected to the servers used for the election data processing.

The SEC has also established cooperation with the Ministry of Public Administration, Digital Society and Media, through which it should obtain licenses for the SQL database and Windows server. However, most of the planned system upgrades depend on the financial resources allocated to the SEC for these purposes.

When it comes to Municipal Election Commissions, it is important to emphasize that most of them do not have separate office spaces. Instead, their offices are located in other buildings. For example, the MEC Niksic is located in the building of the Municipality of Niksic and does not have its own IT infrastructure. The MEC is under SEC control during the parliamentary and presidential elections, which means that they must use software solutions that the SEC instructs them to use. The SEC also trains MEC members in the use of election data processing software. According to our interlocutor from the SEC, training in the use of software takes less than an hour, where most of the time is spent introducing the user to the way the VPN works. However, when it comes to local elections, the SEC cannot control which software is used by the MEC. The MECs are responsible for conducting all election activities in local elections, including the selection of software. This is another in a series of problems that could be solved with a legal provision stipulating that parliamentary and local elections be held on the same day in all municipalities.

# RECOMMENDATIONS

1. It is necessary to provide adequate funds to the State Election Commission for modernization of IT infrastructure;

2. Amendments to the Law on the Election of Councilors and MPs must enable the presence of an additional electronic device at the polling station, for the purposes of using software for processing election material. At the same time, it is necessary, in cooperation with IT experts, to prescribe in the Rulebook the manner in which the device would be configured, the exact moment of activation of the device at the polling station, the person responsible for use and his/her deputy;

3. The State Election Commission, which is in possession of the source code of the software that OSCE has donated, must work on improving the software module for verifying signatures for the support of electoral lists, so as not to violate the provisions of the Law on Data Protection;

4. The State Election Commission should provide all employees with regular training on cyber security;

5. Reduce the number of signatures required for the confirmation of the electoral list with the introduction of mandatory verification of the authenticity of signatures by notaries. Also introduce a limit on the price of this service so that it is not a limiting factor for the nomination of candidacies;

6. Before using the software for processing election data, it is necessary to conduct a cyber attack simulation, in order to test the cyber security of the State Election Commission. The possibility to provide support to the SEC by the Service for IT Security and Technical Supervision Systems in the Ministry of the Interior should also be considered.

# ABOUT CEMI

The Centre for Monitoring and Research – CeMI is a nongovernmental, non-profitable organization, founded in March 2000, whose main goal is to provide infrastructural and expert support for continuous monitoring of the overall process of transition in Montenegro.

CeMI has been monitoring elections in Montenegro, as well as other countries, for 20 years, through membership in the European Network of Election Monitoring Organizations (ENEMO). By implementing the project of civic election monitoring, CeMI strives to contribute to democratic conditions for holding transparent, free and fair elections through civic control of the electoral processes in Parliamentary and Local elections.

During its long and consistent work CeMI has contributed to changing social and political circumstances in which it was created, and consequently expanded the scope of its work towards legislative initiatives, public opinion polls, fight against corruption and respect of human rights and freedoms.

Amendment of the constitutional status and progress in the European integration process have positively impact the development of civil society in Montenegro, giving it an entirely new framework of the work. In that context, CeMI deviates from the work of regular non-governmental organization and is getting closer to the concept of a research center for the creation and representation of policy proposals.

CEMI is a Think Tank organization whose mission is to continuously provide support to reforms and strengthening of the institutions of the political system and civil society organizations through proposing and monitoring the implementation of public policies in the field of human rights and freedoms of European integration and fight against corruption in Montenegro.

CeMI would like to thank the British Embassy in Podgorica, who financially supported the Project of Civic Election Monitoring and facilitated this mission. CeMI also wishes to express its gratitude to all representatives of the election administration, state bodies, political societies, international observation missions and domestic nongovernmental organisations, with whom a cooperation was established in the implementation of this mission.