POST-ELECTORAL REVIEW CONFERENCE

EARLY PARLIAMENTARY ELECTIONS IN THE REPUBLIC OF MOLDOVA:
LESSONS LEARNED, RECOMMENDATIONS AND STEPS AHEAD

28 October 2021, Session on Alternative Voting Methods

Alternative voting methods:
Good European practices and steps to be taken

Contribution by Ardita DRIZA MAURER
Expert, Venice Commission, Council of Europe

General principles

The Moldovan CEC is considering introducing alternative voting methods, namely internet voting, to offer Moldovans abroad an effective channel for participating in elections. This presentation very briefly outlines the main Council of Europe and Venice Commission standards in this field.

All solutions employed during elections, including solutions based on the use of information and communication technologies (ICT) such as internet voting, should respect several *principles and conditions of free and democratic elections*, namely the right to universal, equal, free, direct and secret suffrage, periodic elections and their publicity and the conditions for implementing these principles, such as procedural guarantees of impartiality, transparency and observation[1] as well as other relevant rights and freedoms.

The exact meaning of the electoral principles which are common to the Council of Europe region is explained in the 2002 Code of Good Practice on Electoral Matters and the 2007 Code of Good Practice on Referendums of the European Commission for Democracy through Law (Venice Commission). These two documents are considered as a benchmark by national authorities and by the European Court of Human Rights, e.g. when interpreting article 3 of the additional (first) Protocol to ECHR (P1-3) on the right to free elections.

The *use of ICT in elections* makes it necessary to consider additional legal instruments which are outside the strict field of elections but are relevant to the ICT used. The Council of Europe Convention on Cybercrime (Budapest Convention) or the Council of Europe Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+) as well as the EU corresponding instrument, the General Data Protection Regulation (GDPR)[2] are examples of relevant instruments. EU standards on cybersecurity,[3] opinions, observation reports, and other documents on the use of ICT in elections, by Venice Commission, OSCE/ODIHR, Council of Europe's Parliamentary Assembly (PACE), etc. are relevant too.

[1] Venice Commission, Code of good practice in electoral matters, Opinion No. 190/2002, adopted by the Venice Commission at its 52nd session (Venice, 18-19 October 2002); CDL-AD (2002) 23 rev.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), applicable across the European Union since 25 May 2018.

[3] For example, EU the 2016 Directive on the security of network and information systems (NIS Directive) which is the first piece of EU-wide legislation on cybersecurity or the EU Cybersecurity Act adopted in 2019 which introduces, for the first time, an EU-wide cybersecurity certification framework for ICT products, services and processes.

Council of Europe detailed standards on e-voting : CM/Rec(2017)5 and Guidelines

According to P1-3 ECHR, the legislator has the task to actively introduce regulations that ensure that only digital solutions which comply with the higher-level principles can be used in elections. *The question is how to write such regulations?* How to translate the general principles into detailed requirements and make sure that technology complies with such requirements and, ultimately, with the principles? The Council of Europe has done pioneering work offering guidance on the application of electoral principles to use of ICT in elections.

The Council of Europe is *the only international organization to have issued recommendations on regulating the use of e-voting*. The 2004 Recommendation on legal, technical and operational standards for e-voting (Rec(2004)11) and the Guidelines on certification and on transparency were more recently replaced by Rec (2017)5 on Standards for e-voting and the Guidelines on its implementation. Rec (2017)5 defines *e-voting as the use of electronics to cast and, or count the vote*, covering both e-voting in *controlled environnements* (electronic voting machines or scanners to count paper ballots) as well as the use of internet voting which takes place in an *uncontrolled environment* (e.g. home, office, etc.), on a device uncontrolled by electoral authorities (e.g. a personal computer) and is transmitted via the internet – a channel outside the control of the authorities.

Rec(2017)5 on standards for e-voting includes *recommendations* which refer to some 49 *standards* (enlisted in appendix 1), an *Explanatory Memorandum* which clarifies their meaning as well as a separate document - the *Guidelines* on the implementation of the provisions of the Recommendation Rec(2017)5. The guidelines are expected to be completed and developed, whereas the Recommendation is meant to be a stable document.

The 49 standards enlisted in the Rec(2017)5 set *objectives that internet voting should fulfill* to comply with the principles and conditions for democratic elections. The standards are meant to offer *guidance to national authorities when regulating the use of e-/i-voting*. Another practical resource is the OSCE/ODIHR Handbook for the observation of new voting technologies.[4] The Council of Europe also provides a *forum for regular discussion* between national experts in the form of biannual meetings to evaluate the implementation of the Recommendation. The next evaluation meeting will take place in November 2021.

To be noted, the Recommendation only includes *minimum standards* applicable throughout the CoE region. Compliance with them can be seen as a first step to ensuring constitutional compliance of internet voting. Member states should, in addition, pay attention to implementing principles which may be specific to their country and to the election in question.

[4] https://www.osce.org/odihr/elections/new_voting_technologies

Good practice and suggested steps when envisaging the introduction of internet voting

Below we outline some legal questions that arise when considering internet voting and suggest answers based on Council of Europe standards and good practices.

First, it is important to consider ***what is the required minimum level of implementation of electoral principles.*** What is for instance the minimum level of secret or of free suffrage that internet or postal voting should provide? What if they enable the voter to sell her vote? What if an infected personal computer/"smart" device from which the vote is issued reveals the content of the vote to a third person without the voter noticing it, etc.?

Secret and free suffrage cannot be ensured when voting takes place in uncontrolled environments; the only way to ensure them is well-organised voting in polling stations. Hence, the general recommendation is that voting from uncontrolled environments can only be envisaged where ***coercion and family voting are not perceived to be an issue***, in so called mature democracies (this is thought to be the case for instance in Switzerland). However, even in such situations, lawyers and judges argue that pressure and coercion may re-appear anytime depending on the issue submitted to vote/at stake. Furthermore, they may be re-introduced by "new" voters (e.g. naturalized foreigners) coming from regions where family voting and coercion are an issue. Lack of secrecy combined with low civic awareness may incentivise vote selling and buying. Hence, countries like Norway and Estonia link(ed) the use of internet voting to the introduction of the ***possibility to vote several times***, the last vote cancelling the previous one, and eventually voting at the polling station, the paper vote overriding any previous e-vote/s. Furthermore, according to the Rec(2017)5 the system should ***not offer the voter proof of her vote for use by third persons***.

Securing the i-vote during transmission requires encryption. However, this is not enough. State-of-the-art requires that internet voting provides for ***individual verifiability***: the system enables the voter to check that her vote is cast, transmitted and registered as intended. The voter receives prior to the vote, through ***a channel independent of the voting one,*** individual verification codes for all possible choices. She refers to such codes to check that her vote was eventually registered as intended. Individual verifiability helps detect any possible change of the vote. In case there has been such a problem, the voter should be able to vote through another channel. It is thus recommended that ***internet voting is used as an additional voting channel***, meaning that it should not be the only voting channel.

A two ways internet voting requires a well-established and well-functioning system of identification and authentication of voters. It further requires accurate voters' registers and synchronisation between registers that track the use of voting rights through different channels allowing to detect and fight multiple voting attempts.

To the difference of other channels, where potential problems are possibly limited to a certain place/part of the electorate, internet voting – if not secure – may allow adversaries to hack the entire e-ballot box and thus greatly impact the election results. In addition to individual verifiability, state of the art internet voting should also provide ***universal verifiability*** allowing anyone to check, through cryptographic means, the correctness of the final result.

State of the art verifiability solutions however rely on cryptographic means. Courts in some countries (Germany and Austria) have considered that the individual voter (in Germany) or the member of the electoral commission (in Austria) should be enabled to ***understand the system and check the results without technical assistance***. Other countries (e.g. Estonia or Switzerland) accept to rely on experts, provided that the voter has the choice to select her trusted expert. The question merits to be discussed and decided at the national level.

Once these and the other legal considerations have been pondered, there are some steps recommended to be taken in view of introducing internet voting, including the following:

1. Inform and involve stakeholders in thinking out the future use of i-voting; identify needs and expectations; elaborate a strategy and be transparent about it.
2. Conduct feasibility study.
3. Introduce regulation of the testing phase. Involve IT, legal and social science research.
4. Procure and approve a prototype.
5. Conduct small scale trials, starting with lower level elections.
6. Evaluate the trials based on well-defined criteria.
7. Decide about the future: redesign and/or extend trials; complete rollout; abandon.
8. If, after the piloting phase, the decision is taken to pursue the use and development of i-voting, then it is recommended to:
9. Clarify and complete the legal basis: introduce detailed regulation for the extended trials or of the complete rollout. Involve IT, legal and social science research.
10. Procure and approve the ICT solution.
11. Regulation should address legal and technical requirements, including functional and non-functional ones. It should address, among others, how integrity and authenticity, availability and reliability, secrecy and confidentiality, usability and accessibility of the system and its functionalities are ensured. It should furthermore address evaluation and transparency requirements, the role of public authorities and of private sector providers.

12. Risks should be identified and evaluated based on predefined criteria. Despite all due care, there are remaining risks when ICT is involved. These should be addressed in a risk management policy framework.
13. Dispute regulation elements (proof, remedies, etc.) should be re-considered and completed, in the light of internet voting.
14. Measures to be introduced in case of incidents, including information and communication ones, should be identified.
15. I-voting system should be regularly evaluated to confirm its constitutional compliance as related risks evolve and the system itself undergoes major changes.
16. Evaluate sustainability.
17. Inform and train the public and stakeholders, especially before an election.
18. Be transparent about all aspects of the use of i-voting to instil trust. Require that only state of the art i-voting solution is used.