INTERNET VOTING THE REALITY OF OUR TIMES

elf

| Victor Guzun | Kevin Tammearu | Ana-Maria Stancu | Alexandru Balmoș |

INTERNET VOTING
THE REALITY OF OUR TIMES

Brussels | Chisinau | Bucharest | Tallinn | 2020

CIP description of the National Book Chamber

Internet voting: The reality of our times / Victor Guzun, Kevin Tammearu, Ana-Maria Stancu, Alexandru Balmoș; editor: Judy Goldman; coordinator: Sergiu Boghean; European Liberal Forum (ELF). – Brussels; Chisinau; Bucharest; Tallinn: S. n., 2020 (Tipografia “Sirius”). – 40 p.: il.

Bibliographic references: p. 39 (9 tit.) and in footnotes. – Appears with the support of Friedrich Naumann Foundation for Freedom, Office for Romania and Republic of Moldova.

– 300 ex.

ISBN 978-9975-57-294-1.

342.843.5:004.738.5

I-58

Publisher

European Liberal Forum asbl
Rue d'Italie 11-13, boite 6
1050 Ixelles, Brussels (BE)

Coordinator:

Sergiu Boghean

Editor:

Judy Goldman

Design and layout:

Roman Burlacu

Contacts

+32 (0)2 669 13 18
info@liberalforum.eu
www.liberalforum.eu

Authors:

Victor Guzun
Kevin Tammearu
Ana-Maria Stancu
Alexandru Balmoș

Cover Image:

Shutterstock

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 46 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard.

ELF was founded in 2007 to strengthen the liberal and democrat movement in Europe. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European.

We bring together a diverse network of national foundations, think tanks and other experts. At the same time, we are also close to, but independent from, the ALDE Party and other Liberal actors in Europe. In this role, our forum serves as a space for an open and informed exchange of views between a wide range of different actors.

Published by the European Liberal Forum asbl, with the support of Friedrich Naumann Foundation for Freedom, Office for Romania and Republic of Moldova and the cooperating partners: Laboratory of Initiatives for Development (LID Moldova), E-CIVIS Association (Romania) and Liberal Institute for Political Analyses (LIPA Bulgaria). Co-funded by the European Parliament. Neither the European Parliament nor the European Liberal Forum asbl are responsible for the content of this publication, or for any use that may be made of it. The views expressed herein are those of the author(s) alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum asbl.

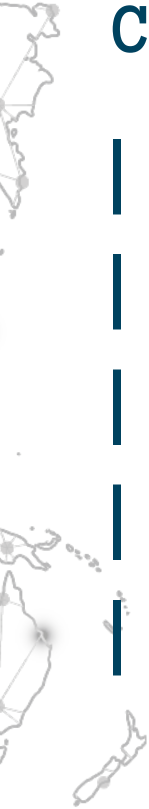
FRIEDRICH NAUMANN FOUNDATION For Freedom.
Romania and Moldova

LIDMoldova
LABORATORY OF INITIATIVES FOR DEVELOPMENT

ecivis

ЛИПА

TABLE OF CONTENTS



FOREWORD

The partnership between the European Liberal Forum (ELF) and the Friedrich Naumann Foundation for Freedom (FNF) in digitalization and public administration reform began in Southeast Europe as early as 2015 when in a joint project we talked about “Liberal reforms for public administration in Moldova.” Back then, together with a mayor and a chairperson of the Estonian County Council, we went to Chisinau and Nisporeni to discuss the benefits of public administration digitalization with local elected officials. Of course, we did not stop there. Two years later, ELF and FNF analysed the electronic reforms carried out in Bulgaria and Romania and compared them with those in Estonia, aiming at “redesigning public services for the 21st century.”

The Friedrich-Naumann-Foundation continued on this path in various projects with its main ally from the outset the former Ambassador of the Republic of Moldova to Estonia, Victor Guzun. He has mediated the dialogue with Estonian specialists over time. Private and state dialogue partners as well as politicians and journalists from

Southeast Europe had the opportunity to learn about good practices in e-health, e-business, e-education, e-government and e-democracy. And it is in the last area that Estonia offers an almost unique service worldwide for its citizens: electronic voting via the Internet.

Thus in the 2019 European Parliamentary elections, around 50 per cent of Estonian citizens used this service. This caught our attention, because I-voting could be a solution in the future for millions of citizens living abroad, especially for the diaspora in Eastern Europe for whom access to this basic democratic exercise is much more difficult. This was true for thousands of Romanian voters in the first round of last year's presidential elections when the polling stations in London, Paris, Madrid and Berlin could not cope with the large inflow of voters. We and ELF deemed this solution for citizens as worthy of consideration as early as last year. Who could have known back then the significance the project would acquire in these pandemic times in addition to its important internal dimension.

Conversations with European experts in voting systems and security, with liberal European politicians, with partners in Romania, Moldova and the diaspora showed us that although interest in this system may be scant in Western Europe, in the East it is high. Nevertheless, factors such as lack of trust in state actors, general distrust of politicians, lack of political will and possible cyber security risks can and probably will be the main obstacles delaying this process for many years, even if all dialogue partners agree on the need to introduce such a system, “at some point when it is safe.”

Thus, without downplaying the fears listed above, in the spirit of the consensus on the need to introduce such a voting system in the future, this publication seeks to provide answers to the questions, arguments and positions raised by our dialogue partners.

Sincerely,

Raimar Wagner, Project director, Friedrich Naumann Foundation for Freedom, Office for Romania and Republic of Moldova

INTERNET VOTING – GENERAL CONSIDERATIONS

By Victor Guzun
e-Governance expert at the Laboratory of Initiatives for Development (LID Moldova).

- **e-Transformation is the reality of our times.** It brings efficiency, effectiveness, and economies of resources in many sectors of our lives. The current pandemic emphasizes the use of e-governance solutions across the world; one of the most discussed issues is electronic voting. In this brief essay, I will describe the basic principles of electronic voting; existing types, benefits and concerns; the Estonian Internet voting system (the only country that has introduced I-voting for all types of elections); and examples of the use of electronic voting from various countries, including failed attempts. I have used multiple sources including the Estonian Electoral Office (EEO)[1], the International Foundation for Electoral Systems (IFES)[2], the International Institute for Democracy and Electoral Assistance (IIDEA)[3], and the European Parliamentary Research Service (EPRS)[4].

- **People have always voted.** It is indeed difficult to make decisions that influence community life without being able to accurately quantify the preferences of the members of the community. In ancient Greece, citizens used pieces of broken pottery on which they scratched the name of candidates for ostracism (exclusion for a period of 10 years). As many as 6,000 votes were needed to exclude an individual. The same procedure and number of votes were applied to welcoming potential new citizens[5]. In ancient India, palm leaves were used for “municipal” elections. A leaf with a candidate’s name was put inside a mud pot to be counted. The term ballot comes from the word “ballotta,” a small ball for voting used in the polling system of the Doge of Venice starting in 697 AD. The first use of paper ballots appears to have been in ancient Rome in 139 BC[6].

After more than 21 centuries, mankind continues to use paper ballots even though much of the data transfer in the world is digital, the volume of data increases every day, and every individual on this planet has the hypothetical possibility to connect and exchange data instantly with any other individual or

[1] For more information: Estonian National Electoral Committee https://www.valimised.ee/en/internet-voting/internet-voting-estonia

[2] For more information: International Foundation for Electoral Systems https://www.ifes.org, last accessed: November 2020

[3] For more information: Institute for Democracy and Electoral Assistance https://www.idea.int/our-work/what-we-do/elections, last accessed: November 2020

[4] For more information: European Parliamentary Research Service https://www.europarl.europa.eu/at-your-service/en/stay-informed/research-and-analysis, last accessed: November 2020

[5] Lang, M. The Athenian Citizen, Democracy in the Athenian Agora. 2004. http://www.agathe.gr/democracy/practice_of_ostracism.html

[6] Jay S.Coggins and C.Fererico Perali, Public Choice, 1998, https://www.apec.umn.edu/sites/apec.umn.edu/files/64-majority-rule-in-ducal-venice.pdf

institution via the Internet. Mankind is now going through a metamorphosis where distance no longer plays a decisive role and data is shared in a split second everywhere. Short-term and permanent migration are common in the globalized world, and modern communication technologies connect people with their own countries and the institutions they represent more simply, more cheaply, and more rapidly than before. People are no longer highly dependent on their places of residence and increasingly demand more open and transparent public services.

The right to vote is one of these services. Speaking of the parliamentary elections in the Republic of Moldova and the e-presidential election held in Romania, many voters in diaspora found their voting rights limited due to long distances to polling stations[7]; high travel costs; the small number of polling stations; limited human, financial, and technical capacities for organizing elections; and bureaucratic procedures or participation restrictions. Tens of thousands of people waited hours in front of polling stations without getting to vote. According to an IMAS study, 63% of the diaspora support the idea of electronic vote.[8] For these reasons, the adoption of I-voting meets the needs of the modern democratic world and is a 21st-century imperative.

WHAT IS ELECTRONIC VOTING? WHICH TYPES EXIST?[9]

1. Optical scanning of the ballots.

Voters go to polling stations, fill out their ballots in ink, and insert the machine-readable ballot into an optical scanner. The scanner analyses the voter’s choice and calculates the data for all voters. For voters, there is no big difference compared with traditional voting procedures. For electoral workers, the process of counting and tabulating votes is much easier and quicker. In case of possible machine malfunctions or recounts, the paper ballots are kept by electoral authorities. The first country that introduced this system was the USA back in 1962.

Photo: Optical scanning of ballots [10]

[7] Adina Pancu, Mediafax, 2020 https://www.mediafax.ro/social/andreea-si-mircea-au-mers-cu-masina-de-la-paris-la-zalau-sa-voteze-19580570

[8] For more information: Diaspora Barometer, IMAS https://imas.md/pic/uploaded/barometrul%20diasporei.%20sondaj%20imas.pdf, last accessed: November 2020

[9] Htet Ne OO , A Survey of Different Electronic Voting Systems, Htet Ne OO, 2014 https://www.researchgate.net/publication/321431416_A_Survey_of_Different_Electronic_Voting_Systems

[10] Photo source: https://bluedelaware.com/2017/12/18/replacing-delawares-voting-machines/

2. Direct Recorded Electronic machines (DRE).

DRE machines are complex electronic devices that work without a paper ballot. Instead of the traditional ballot and use of a pen or stamp, voters push a button or use a touch screen to select their candidates. The first machines were introduced in 1975 in the USA.[11] The absence of paper ballots makes the electoral process easier as there is no need to design, print, keep and transport them during an election. The machines used in various countries differ, from the very simple and robust systems used in India[12] for almost one billion voters to elaborate models with multilingual interfaces, different font sizes, and even movement sensors for people with disabilities. DRE machines are the most-used electronic voting options worldwide (as described in the last chapter). The big disadvantage of the DRE method is that there is no physical proof of the vote, so the confidence of the voters is not fully assured. To solve this problem, some modern voting machines print and store voters' choices.

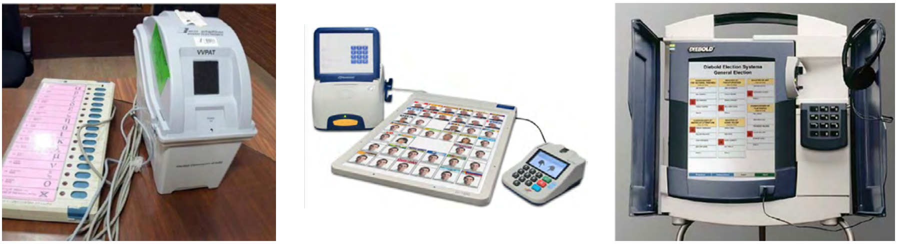


Photo: DRE machines used in India, US, and Venezuela.[13]

3. Internet voting.

This voting method allows voters to vote remotely from any location in which there is an Internet connection without the need to visit a polling station. All phases of the electoral process are online using secure identification methods and tools. It has been developed in various countries,[14] but so far only Estonia uses this system for all types of elections: local, parliamentary, and EU Parliament.

Photo: Estonian e-ID, used for internet voting[15]

[11] For more information: Pros and Cons on Controversial Issues https://votingmachines.procon.org/historical-timeline/, last accessed, November 2020.

[12] For more information: Election Commission of India https://eci.gov.in/evm/, last accessed: November 2020

[13] Photo source: https://elections.smartmatic.com/venezuela-leads-the-way-in-electoral-best-practices-worldwide/; https://www.thehinducentre.com/the-arena/article24818243.ece; https://www.geekwire.com/2016/microsofts-windows-ce-powers-u-s-touch-screen-voting-systems-causing-concern-among-security-experts/

[14] For more information: See the list in the end of the article, last accessed: November 2020

[15] Photo source: https://news.err.ee/963141/interview-how-e-voting-works-in-estonia

STANDARDS FOR ELECTRONIC VOTING

As in all types of elections, electronic voting standards should comply with the International Covenant on Civil and Political Rights adopted by the United Nations in 1966[16], namely universal and equal suffrage and secrecy of the vote. There are no internationally adopted standards for electronic voting or voting technology at the moment, so they vary from country to country. In 2004, the Council of Europe adopted a recommendation[17] on standards for electronic voting comprising the following main principles: voters should be reliably identified; have the chance to confirm their choices before they vote and the ability to check that the vote was correctly cast after voting; the vote should be anonymous; and all aspects of the electoral process must be fully transparent, easy to understand and use.

BENEFITS OF ELECTRONIC VOTING

1. Convenience.

Electronic voting is quick, precise, and based on very accurate, quickly updated digital electoral lists. Internet voting allows citizens to vote from any location with an Internet connection, making this method very efficient for large communities of expats, for citizens living abroad permanently, and for travellers and saves lots of time and resources too.

2. Increased turnout.

Electronic voting increases the possibility to vote for a larger number of citizens. As the average percentage of people participating in elections is constantly decreasing around the world, electronic voting—especially Internet voting—could help to increase turnout and therefore make election results more appropriate and representative. The lack of voting opportunities for millions of citizens living abroad is a serious problem for many democracies. For example, only 48.54% of citizens with the right to vote participated in the presidential election on 1 November 2020 in the Republic of Moldova (the first round) compared with 50.95% in the 2016 election[18].

3. Saves money and resources.

In Estonia, Internet voting costs per person are almost ten times less than traditional paper ballot voting costs and saved 11,000 working days during the 2017 elections.[19] Once introduced, Internet voting is a cheap and convenient means for suffrage, especially in countries with frequent elections and referendums, also keeping in mind that many voters might have to travel substantial distances taking up lots of their time to cast their votes on election day.

[16] For more information: International Covenant on Civil and Political Rights, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, last accessed: November 2020

[17] For more information: International Covenant on Civil and Political Rights, https://www.ohchr.org/Documents/Professionalinterest/ccpr.pdf last accessed: November 2020

[18] For more information: National Election Committee of the Republic of Moldova https://cec.md, last accessed: November 2020

[19] Dario Cavegn, Estonian National News Broadcaster ERR, 2018 https://news.err.ee/863027/scientists-calculate-administrative-cost-to-state-of-electronic-votes

4. Voter registration.

Digital voter registers are very accurate and can reflect last-minute information extracted from population registers. Therefore, in the majority of the cases, they exclude deceased people, avoid double registrations, and decrease the possibilities for electoral fraud. In contrast, electoral rolls on paper are less protected against these risks and as a result are less credible. Biometric data collected from citizens also decreases the possibilities for incorrect voter registration.

5.Voter identity verification.

Multiple voting is a serious problem in many countries; digital solutions can help to decrease this phenomenon. Using secure digital identification tools, on election day election workers could check the identity of the voter and compare it with the electoral list, using updated information from the population register. In Estonia, identity is checked remotely via secure e-ID cards and infrastructure available to any registered resident. In several countries, biometric data is used to compare the identity of the voter against electoral lists.

6.Vote casting.

Electronic voting helps to overcome many problems associated with actually casting a vote. In Estonia, the entire voting procedure takes few minutes. The interface is easy to use and understand and voters can redo the procedure if they made a mistake or change their preference or even if their vote was forced. In some countries, illiteracy is a serious problem, and DRE machines make the choice easier for voters. Electronic voting can also help disabled people to vote if they cannot travel to the polling station on election day or if they have visual impairments.

7. Vote counting.

After the polling stations are closed, the scrupulous process of vote counting starts; digital counting is very quick and accurate and practically eliminates human error and substantially reduces the need for human resources. This is particularly important in large countries like India, the US, and Brazil. The procedure for counting Internet votes in Estonia is almost fully automated and very quick.

8. Tabulation and transmission of results.

Countries open thousands or even millions of polling stations for every election. Collecting all the results from all polling stations and constituencies can be a very complex, lengthy process and in some cases, a not very precise one. Digital tools allow for instantaneous transmission of secured data which means a quicker tabulation and announcement of the results.

MAIN CONCERNS OF ELECTRONIC VOTING

1. Trust.

This is the biggest concern of voters, state institutions and political parties about electronic voting. Often people and even political leaders find electronic election systems difficult to understand and their first reaction is to stop using them. Claims of malfunctioning systems could be and are often used by different politicians in various ways for various ends. In many countries, lack of trust in e-election systems has led to serious resistance and as a consequence, interruptions in their implementation (see the last chapter). Building trust in e-elections is a gradual matter that depends on the general level of trust in state institutions. Many experts suggest that introducing electronic voting gradually would be best.

2. Protection from electoral fraud.

Electronic voting is a democratic procedure but irresponsible or corrupt country authorities could use digital solutions to influence election results either intentionally or mistakenly.

3.Reliability, auditability, and verifiability.

Electronic identification is not always fully accurate, the systems do not work properly all the time, and Internet connections and hardware malfunctions occur in many places, especially in undeveloped countries. If voting is only digital, there is serious concern about how to check the accuracy afterwards in cases of electoral fraud, recounts, or mistrust. To overcome this problem, some DRE machines are designed to print a paper copy of the vote known as a VVPAT (voter-verifiable paper audit trail). Once their votes are cast electronically, many voters do not know what happens to them in the voting machines or if their votes were properly recorded and counted. The newest e-voting systems allow voters to check their votes using the E2EVV system (end to end verifiable voting)[20], which allows voters to verify that their vote was cast, recorded and counted correctly. The Estonian remote voting system has allowed voters to use the E2EVV system since 2013.

4.Testing and certification.

This is a concern due to the fact that if the systems are not properly tested and certified, they tend to have insufficient credibility. For many people, electronic voting technologies and their functionalities are not well known, therefore testing and certifying these systems by independent and credible entities is essential. For example, Estonia regularly tests[21] the hardware and software components of their election systems. In some cases, independent entities have managed to interfere in the work of various systems which undermined their credibility.

[20] Martin Russel, Ionel Zamfir, European Parliamentary Research Service, 2018 https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf

[21] For more information: Estonian Information System Authority https://www.ria.ee/en/news/e-voting-too-secure.html, last accessed: November 2020

- **5.High costs.**

  In some countries, the implementation of electronic voting technologies could be a costly affair. DRE machines are complex, expensive, and hard to maintain in working condition and difficult to store between elections. Some countries might have to change their secure identification certificates if, for example, if they wanted to issue e-ID identification cards to every citizen following the Estonian example. Last generation hardware and computers and computer literacy programs could be also quite expensive.

Materials from Considerations on Internet Voting: An Overview for Electoral Decision-Makers were used for this chapter[22]

How I-voting works in Estonia[23]

Estonia is the only country in the world where 99% of the public services are available online 24/7 (except for marriages and divorces, so far). Thanks to a safe, convenient, and flexible digital ecosystem, Estonia has reached an unprecedented level of transparency in governance and has built broad trust in its digital society [24].

I-voting allows votes to be cast via the Internet from anywhere in the world where there is an Internet connection. A computer with an Internet connection, an Estonian ID-card (mandatory for all citizens), or a mobile ID (downloaded on your phone) with valid certificates are required.

Both the ID-card and the mobile ID have a 4-digit ID for user access to the I-voting system and a 5-digit code used for digital signature authentication, which is also used for the final authentication of the I-vote.

I-voting is organized by the Estonian Electoral Office in cooperation with the Information System Authority. Before voting begins, the State Electoral Office prepares the I-voting system and posts it on the Electoral Office website. Electronic voting is open 24 hours during the 7 days of early voting (from the tenth to the fourth day before election day). To vote, this application needs to be downloaded from the office website to the user's computer. After downloading, the user enters the electronic election system using the 4-digit code on the ID or mobile-ID. Once the system recognizes the user, the integrated system connected to the population register database recognizes the citizen's or resident's eligibility to vote (local, parliamentary, or EP elections) and based on the user's residence, displays the lists of candidates for that district. Once the user chooses the party or candidate for which he/she wants to vote, the vote is encrypted, and the system requires the application of the 5-digit digital signature code. The entire voting procedure takes on average 2 minutes.

[22] Meredith Applegate, Thomas Chanussot, Vladlen Basysty. Considerations on Internet Voting: An Overview for Electoral Decision-Makers, 2020. https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

[23] For more information: Estonian National Election Committee https://www.valimised.ee/en/internet-voting/general-framework-electronic-voting, last accessed: November 2020

[24] Federico Pantera, E-Estonia Briefing Centre, 2018 https://e-estonia.com/cornerstone-governance-trust/

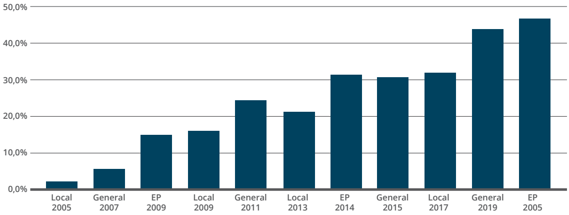
After the digital signature is applied, the encrypted vote is forwarded to the vote collecting server and the user receives a vote confirmation along with a QR code that sets the exact time when the vote was forwarded to that server. I-votes are encrypted using an up-to-date crypto-algorithm. The precise specification of the algorithm is determined by the Electoral Office before every election. A vote is encrypted with the help of two encryption keys: for public application and vote-opening application. The latter can operate only with the help of several keys distributed to the members of the National Electoral Committee.

To avoid third parties influencing a user's voting option, multiple voting is possible. Only the last I-vote cast is taken into account, and earlier votes are annulled. As an additional security measure, a vote cast on a ballot paper in a polling station on election day or during early voting (4 days before) will annul earlier electronic votes. Before election day, the voting district committees receive the lists of voters who have voted electronically to avoid double voting. The I-votes of citizens who voted by paper ballot are automatically annulled.

- **Counting I-votes and verifying results.** The procedure is public, and members of the National Electoral Committee are present. Personal data are separated from electronic votes (a system of 2 electronic envelopes is used). An I-vote contains only the election identification and a candidate registration number. I-votes are publicly opened using a set of different access keys. Access to the keys is distributed among the members of the committee, and the results are entered into the election information system. The results of electronic voting are not published until the closing of the traditional ballot boxes so as not to influence voting options.

After counting I-votes, their integrity is checked via a second recount in which the electronic votes are mixed in such a way that the decryption of both the input and the output will give the same result. Auditors and observers can check the anonymity and correctness of voting.

- **Level of participation in I-voting.** The system was first used at the national level in the 2005 local elections; in all, 11 internet elections have been organized so far. The share of I-votes has steadily increased in all types of elections starting with 1.9% of the total number of voters in 2005, and culminating with 46.7% in the latest European Parliamentary elections[25] (May 2019).



I-voters among participating voters

Source: Estonian Election Committee [26]

[25] For more information: Estonian National Election Committee https://www.valimised.ee/en/internet-voting/internet-voting-estonia, last accessed: November 2020

[26] For more information: Estonian Election Committee, https://www.valimised.ee/en/internet-voting/signed-results-electronic-voting, last accessed: November 2020

COUNTRIES THAT USE OR HAVE PILOTED INTERNET VOTING[27]

Estonia: This is the only country to allow all citizens the option of online voting in local, national, and European elections.

Norway: Online voting for 2011 local and 2013 national elections was made available in some districts. In 2014, I-voting was discontinued for security reasons.

Switzerland: Some cantons offer online voting to overseas voters (and in a few cases to resident voters) in elections and referendums. The ultimate goal is to roll out I-voting to the entire country.

Armenia: Diplomatic staff and their families can vote online.

Netherlands: In 2004, the country used I-voting for the elections to the Rijland Water Board and in 2006 (for overseas voters) for national elections. I-voting was discontinued in 2007.

United Kingdom: Online voting was trialled in local council elections between 2002 and 2007.

France: I-voting was used for overseas voters in 2012 parliamentary elections but discontinued in 2017 due to security concerns; the government plan is to bring it back in 2022. Overseas residents also voted online in 2016 Republican Party primaries.

Spain: In 2010, Barcelona held an online referendum on a controversial urban development project.

Canada: Online voting is possible in municipal elections in some districts in Ontario and Nova Scotia. Canada is considering introducing I-voting for federal elections.

[27] For more information: E-Voting.cc Team https://www.e-voting.cc/en/it-elections/world-map/, last accessed: November 2020

United States of America: Despite security concerns raised when a District of Columbia trial of I-voting was hacked, 22 US states allow military personnel and overseas residents to vote online.

Mexico: Some states allow online voting for overseas voters.

Panama: Some overseas voters can vote online.

India: In 2010, Internet voting was trialled in local elections in the State of Gujarat.

New Zealand: Overseas voters can vote online.

Australia: Online voting was trialled for overseas military personnel in 2017 but has been discontinued. New South Wales allows some groups (disabled, living in remote areas or out of state) to vote online, but there is no plan to extend this possibility to other states.

● **The reasons for adopting I-voting are obvious.** I-voting erases geographical boundaries so citizens can exercise their voting rights wherever there is an Internet connection without being forced to travel long distances and incur financial expenses or lose time. The greatest possible participation in elections of citizens with the right to vote directly increases the representativeness of elected bodies. Once the system is in place, I-voting is cheap and fast and the financial and human costs involved in the process are small compared to the high costs unavoidable in organizing traditional voting. I-voting is safe and can be verified and counted at any stage if appropriate securing encryption technologies are used. I-votes help to reduce electoral fraud and greatly reduce the risk of manipulation. We can be sure that most democracies will use I-voting in the future. Why don't we start implementing it right now?

COMMON QUESTIONS ON I-VOTING

By Kevin Tammearu
Head of Business Development at Cybernetica, Estonia

Over the past 15 years since Estonia first introduced I-voting [28], online voting has developed into an option that today is on the forefront of advancing our democratic rights. Forward-looking governments that want to give citizens the ability to participate in elections—the democratic decision-making processes—regardless of geographic location have made these efforts around the world. In addition to Estonia, other countries, or regions within them, such as Switzerland, Norway, Australia, and Canada have piloted and implemented Internet voting. Each of these countries implements or pilots a form of online voting that supports key democratic principles such as the universal, free and equal right to vote and to ballot secrecy [29].

Arguably one of the most successful and sophisticated examples of this comes from Estonia where it has been possible to cast legally binding votes over the Internet since 2005. Although several key factors play into the success of the Estonian model such as the existence of unique identifiers (citizens' ID-codes), a mature digital identity ecosystem largely based on these unique identifiers and—at the time—a favourable political climate, the adoption and wide-spread use of Internet voting has not been without its challenges.

Even if the idea of Internet voting might sound like a relatively direct implementation of Internet-based technologies and practices in the context of elections, those at the forefront of implementing I-voting have seen a great deal of opposition, especially political opposition. This has been true in Estonia where during several election cycles the Centre Party, then the biggest opposition party, politically dissented against the process.[30]

And this shouldn't come as a surprise since our traditional, paper ballot elections are also heavily scrutinized, are mission critical in nature and revolve around one of our most treasured democratic rights. And so, with the use of information

[28] For more information: e-Estonia Briefing Centre, https://e-estonia.com/solutions/e-governance/i-voting/ last accessed: November 2020

[29] For more information: The Electoral Knowledge Network, http://aceproject.org/ace-en/topics/vo/introduction/vo20 last accessed: November 2020

[30] Scott Abel, ERR, 2014 https://news.err.ee/112524/government-calls-group-s-criticism-of-national-e-voting-system-unfair

technology, we see issues in several areas such as integrity, transparency and privacy with a potentially higher scale of exploiting the systems in use.

These are largely legitimate fears that the population, voters and citizens in democratic countries can have. It is clear that no IT system is 100% secure and also that no system involving people is 100% secure. In this sense paper ballots, Internet voting and electronic voting all have their merits and flaws, and all of them have the ultimate question of trust hanging over them.

During the 15 years of Internet voting in Estonia, the security of I-voting has been continuously improved upon, and each consecutive vote has been significantly more secure compared to previous one. This is in large part thanks to the scrutiny and criticism levelled at the overall Internet voting approach. The ability for international and national observers to observe and scrutinize the systems in use only strengthens the overall process, as there is a constant driver for improvement [31].

SCRUTINY DRIVES IMPROVEMENT

Criticism of and feedback about I-voting make it possible to improve the overall approach by various means, such as determining and mitigating attack vectors that make it possible to avoid manipulation of results, [32] or reducing dependencies on specific server platforms to avoid and minimize the possibility of someone taking control of them to influence the results [33]. In many cases this can also mean that relevant procedural changes are implemented [34].

After elections there will always be people who doubt the validity of I-votes and who continue to criticise the approach. Informed scrutiny drives improvement; however, some of this can also be the result of the complexity of the underlying technological system and, to someone not well versed in electoral procedures, the general complexity of voting procedures and principles. Some of this can also be the result of political plays and choices. By looking at some of the informed scrutiny the Estonian I-voting model has received and by highlighting the rationale behind its design, governments or agencies considering online voting can build on these lessons.

[31] For more information: OSCE Elections Report, https://www.osce.org/odihr/77557, last accessed: November 2020

[32] For more information: Compendium of Cyber Security of Election Technology, https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf, last accesed: November 2020

[33] For more information: Cybernetica on i-Voting, https://cyber.ee/competences/business-domains/#internet-voting, last accessed: November 2020

[34] Andrew Whyte, ERR, 2019 https://news.err.ee/963141/interview-how-e-voting-works-in-estonia

TECHNOLOGY, PROCEDURE, STRUCTURE AND PROTOCOL

There are a number of functions during elections that need to be covered so that voting goes smoothly. These include technological and procedural elements, organizational structures and interoperability and also protocols that all have to be aligned [35]. The core of the tasks that need to be considered are the following:

1. We will need to identify voters and give access to eligible voters only.
2. Voters identified and eligible should then be able to carry out the voting itself by marking a ballot with the voter's preferences and casting it.
3. It'll be necessary to record the votes that have been cast.
4. These cast votes will need to be stored so that they can later be used for counting the votes.
5. Finally, the votes that have been cast will be tabulated to produce the correct result from valid, cast ballots in accordance with election rules.

Each of these tasks is subject to scrutiny, especially since online voting is primarily an experience in which we cast votes from a remote location over the Internet like the author of this chapter did in the 2019 Estonian Parliamentary elections from Kigali, Rwanda using a laptop and mobile-ID.

For this to make sense from a citizen's perspective, it should be possible to participate in elections using our own devices such as PC's, laptops and perhaps even tablets or smartphones as the voting device.

Now if we also add in the consideration that Internet voting doesn't happen in a physical voting booth where elections officials have oversight possibilities, then based on the tasks mentioned above, we must understand how the eligibility

[35] For more information: Microsoft, https://blogs.microsoft.com/eupolicy/2019/05/10/electronic-voting-estonia/ last accessed: November 2020.

of a voter can be assured, how do we make sure that a voter isn't forced into voting in a certain way and finally, how do we make sure that the vote remains secret and protected. We'll look at these three topics and then continue with some of the most common questions regarding I-voting in Estonia as described by the Estonian National Electoral Committee.

IDENTIFYING A VOTER

The main concern for identifying a voter is how we verify the eligibility of a voter during online voting. This should essentially be based on having unique identifiers and a digital identity ecosystem in place. In the Estonian case, individuals can use their digital identity provided for a number of activities and procedures throughout their lives and not just necessarily for I-voting [36]. This means that there's an existing infrastructure and common practice in place of securely authenticating citizens and providing digital signatures that carry the same weight as hand-written signatures and that can support I-voting use. In Estonia, it is possible to identify a voter reliably in the I-voting system on the basis of a nationally issued identification document which may be an ID-card or a mobile ID. Estonia in this situation is simply one case study with a relatively mature ecosystem [37].

The main point, however, is that I-voting needs a method to check and verify the eligibility of voters; this should be possible regardless of their physical location. This means we need a way to identify eligible voters, distinguish them from non-eligible voters and have means in place for voters to prove their identities, i.e., to prove that they are who they claim to be.

There are two areas of consideration to overcome this challenge:

THE FIRST PART

is related to having strong authentication. This is evident in countries that have digital identity ecosystems that enable citizens to use online services across different domains. These solutions should consider security, usability and enrolment characteristics.

THE SECOND PART

is related to having an up-to-date voter registry that can be interfaced with the voting system. The voting system should be able to query the voter registry and make sure that a voter is eligible.

PROTECTING THE VOTER

Since Internet voting is not dependent on having a monitored voting booth, there is a higher threat of coercion than in polling stations. From this perspective, voters should have some form and level of protection from being coerced into voting for a certain candidate or party and at the same time the assurance that it will be feasible and reasonable to vote over the Internet.

Feasibility in this case means that the measure against coercion should still make it possible to vote over the Internet and not add layers of friction that make it too cumbersome. In this sense, every additional security measure should weigh the benefit it brings against the cost and loss in user-friendliness. After all, we should consider coercion less of a technological problem and rather an element of human behaviour and interaction. From this perspective, the approach to coercion should consider putting in place measures that reduce the likelihood of success by (1) allowing voters to vote several times and only tabulate the last vote and (2) making it possible for voters to vote both on paper and online, in which case paper votes take precedence and will be counted in the results. The latter option works if voter registries are digitalized and there are supporting information systems for voting officials to validate whether the voter has already cast a vote or not.

SECURING THE VOTE

So now that we can identify a voter and have procedures in place that reduce risk of coercion, we also need to have means to secure the vote and ensure ballot secrecy as a fundamental principle of elections [38]. This means that the vote should be secret and protected from disclosure so it is not possible to tell how a voter voted.

The technological means for ensuring ballot secrecy is using strong encryption by using public key infrastructure [39] (PKI), where the election management body [40] generates an election key pair with an election private key and election public key. The latter is then distributed to the eligible voters who use the public key to encrypt their ballots on their devices before casting their votes. These can then be decrypted only by using the private key held by the election management body, which is done before tabulating the voting results.

ELECTION INTEGRITY

To ensure election integrity and maintain trust in the system, it is important that the means for Internet voting provide the intent of the voter and protection from tampering. The main technological approaches for protecting digital ballot boxes and the individual votes within them are digital signatures based on PKI.

[38] For more information: Estonian National Electoral Committee, https://www.valimised.ee/en/internet-voting/introduction-i-voting, last accessed: November 2020

[39] For more information: PKI, https://en.wikipedia.org/wiki/Public_key_infrastructure last accessed: November 2020

[40] For more information: The Electoral Knowledge Network, http://aceproject.org/ace-en/topics/em/ema/ema01 last accessed: November 2020

Digital signatures [41] in this case are meant to ensure authenticity and to protect the integrity of the vote: A digital signature method based on public key cryptography will enable voters to have private keys attributed to them only. Digital signatures in the context of Internet voting are used together with strong encryption to secure the vote and provide integrity. This enables a double-envelope system[42] such as the one used in postal voting.

FREQUENTLY ASKED QUESTIONS BY THE ESTONIAN NATIONAL ELECTORAL COMMITTEE:

- **Security of I-voting**
  Is it safe to vote over the Internet?

I-voting is as reliable and secure as voting in the traditional way. I-voting has taken place since 2005, and the measures to guarantee security have been constantly improved. The following is a brief overview of some of the more important aspects of security.

Since the 2013 elections, voters have been able to check if their votes have reached the election server. Checking their votes by the voters is a new instrument that enables them to verify that their computer behaved correctly and that no malware that may have disturbed I-voting had been installed there. If voters have any doubts that their votes reached the election server, they can file a complaint with the Estonian National Electoral Committee.

Monitoring the work of central voting servers, observing and the auditing conducted by independent auditors are the security measures ensuring that I-votes are stored and counted in the correct way.

The starting point for the construction of an I-voting system was that voting over the Internet should be as reliable as possible. Therefore, it is necessary that voters identify themselves with an ID-card or mobile-ID and do not use any other, less secure solutions for identification. The structure of the I-voting system ensures that nobody can find out whom the voter voted for.

Security is also increased by the fact that the functioning of the I-voting system can be followed and monitored by observers. In July 2013, the source code for I-voting system software was made public for examination and study by all interested on the election web page.

[41] For more information: State Information System Authority, Estonia https://www.id.ee/en/article/digital-signing-and-electronic-signatures/, last accessed: November 2020

[42] For more information: Microsoft, https://blogs.microsoft.com/eupolicy/2019/05/10/electronic-voting-estonia/ last accessed: November 2020

But international experts have found that the system is not reliable, e.g., there has been criticism from the OSCE.

The election managers take the recommendations of international experts very seriously. The OSCE has carried out two full-scale observation missions focusing on I-voting. As a result of these missions, several proposals were made for improving the system, but it was never found that the system was not secure[43].

As it is not possible to compare the Estonian solution with similar solutions in other countries, the criticism of experts (e.g. Halderman [44]) is often based on issues that have already been solved in Estonia.

Can I-voting be secure if internationally several elections (USA, Netherlands have been “hacked”?

In both cases, the voting systems were not hacked: In one case, the e-mail servers were broken into [45], and in the other case, there was a software error in the vote forwarding system [46].

The security of Estonian I-voting is to a great extent ensured by the fact that the infrastructure necessary for its functioning (cards, readers, software) is not designated specifically for elections but is used daily in work procedures, banking, etc. If the Estonian electronic way of life had major technological security holes, it would have been possible to destroy our whole banking system a long time ago, not to speak of the general functioning of the state—we do not even have enough service counters left. I-voting in Estonia is just one of the many e-services provided by the government. Therefore, we can presume that possible technological errors will be detected during everyday use, which is not I-voting. This in its turn adds a sense of security that the change in the operative situation during elections is both monitored and noticed.

RESULTS OF I-VOTING

How can voters be sure that their votes reached the I-voting system correctly?

With the help of a verifying application that can be downloaded to a smart device, each voter can check if the vote that reflects his/her will has reached the I-vote collector correctly. If the vote is not the same, the voter should contact customer service immediately. The vote can be checked for thirty minutes up to three times.

[43] For more information: OSCE, https://www.osce.org/odihr/elections/estonia last accessed: November 2020

[44] Drew Springall and Team, Security Analysis of the Estonian Internet Voting System, 2014https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

[45] For more information: CNN, https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html last accessed: November 2020

[46] Jasper Bakker, Computer Weekly, 2017 https://www.computerweekly.com/news/450424978/Dutch-e-voting-is-waiting-for-an-opportunity

How can you be sure that all collected I-votes are counted correctly and the voting result is right?

Data auditors and each observer who has passed relevant training can check the correct functioning of the system.

The conformity of votes collected, votes to be counted and votes counted is checked by mathematical means within the framework of a data audit to confirm the correct functioning of the process.

How is it possible that voters of advanced ages vote as actively as the young?

In Estonia, the ID-card is used for carrying out everyday transactions; all things necessary for life can be managed with the help of it. Even the aged know how to use the ID-card and the computer. And the number of the aged among the I-voters grows year by year.

Does I-voting favour specific political parties?

Kristjan Vassil and Mihkel Solvak, researchers at the University of Tartu, have reached the conclusion in their work [47] that I-voting does not favour specific political parties. No political party gets an advantage in an election just because some of the voters for that party decided to use another method of voting. They would most probably vote for that political party also without the possibility of I-voting, but if they have been given that possibility, they use it.

VOTING PROCEDURES

How has I-voting influenced voter turnout?

The introduction of I-voting has not had a significant impact on voter turnout. The greatest impact on voter turnout has been in voting in foreign states. Around one third of the voters have decided to use the new voting method or I-voting, and researchers have found that the voters who I-vote are likely to participate also in the next election.

How is it ensured that each voter votes himself or herself (independently)?

I-voting does not take place in a controlled environment like a polling place. In order to ensure that voters express their will freely, they always have the possibility to choose a suitable time and place for I-voting. If voters cannot vote freely, any electronic votes cast may be changed by voting online again during early polling, or by voting at the polling station during early voting. In such a case, the last I-vote cast or the vote cast at the polling place is the one counted. Voters may not change their votes on election day.

[47] Kristjan Vassil, Does Internet Voting Bias Election Results? Evidence from Estonia, 2014 https://www.ut.ee/kristjan.vassil/wp-content/uploads/Bias_report.pdf

How is vote buying / transfer of ID-card and codes prevented?

Buying of I-votes is a crime, like all other forms of vote buying. If it is suspected, the police will deal with it. Vote buying is punishable under § 162 of the Estonian Penal Code, pursuant to which the punishment is a pecuniary punishment or imprisonment. Transfers of ID-cards and codes are prohibited; each person is responsible for safeguarding his/her digital identity.

How is the secrecy of I-voting ensured?

Voter application encodes (encrypts) the voter's vote with the public key in such a way that in forwarding the vote, it is not possible to see for whom the voter voted. Before counting votes, the I-voting system separates the voter's personal data from the vote cast. The votes can be opened only with a secret key, the access to which is divided among the members of the National Electoral Committee. More than half of the members of the National Electoral Committee have to be present to open the votes.

CONCLUSIONS

online voting systems have to support the key democratic principles of enfranchisement, privacy and integrity. To support these objectives, online voting systems need to optimally balance the accessibility, security and transparency that are critical in creating public trust in the system with the legitimacy and credibility of the election process. The underlying technology must support transparent online voting and allow for auditability by officially appointed external parties and individually by voters. Only then is it possible to prove to stakeholders that the online voting system performed its task correctly and that the voting result is legitimate.

CONSIDERATIONS FOR THE INTRODUCTION OF INTERNET VOTING IN ROMANIA

By Ana-Maria Stancu
President of E-CIVIS Association, Romania

Surprisingly for many legislators and stakeholders, Romania used electronic voting via Emergency Ordinance 93 of October 9, 2003[48] regarding voting by electronic means during the national referendum for the modification of the Romanian Constitution. The ordinance was passed to facilitate voting for military personnel and policemen who were employed in foreign missions in Afghanistan, Bosnia-Herzegovina, Iraq and Kosovo at the time of the referendum. Basically, it was a onetime experiment for Romanians voting in military theatres overseas.

Although this was an electronic vote, it was organized in precinct stations. Citizens who participated received a sealed envelope on the premises containing data for accessing the voting system (user name and password) with which they were able to connect and vote on the screen. This was not what we would call a normal electronic vote these days, but nonetheless, electronic infrastructure was used for Romanian citizens abroad to be able to vote.

In 2009, during the negotiations the Pro-Democracy Association (www.apd.ro) was conducting with the parties to modify the electoral laws and introduce uninominal voting, the subject of voting by correspondence and electronic voting was raised, but all the parties opposed it due to lack of trust in this type of voting system.

After several years, and due to a major election scandal that led to the resignation of the incumbent Ministry of External Affairs, in 2015 Parliament passed Law No. 288 [49] that stipulates the means to exercise correspondence voting in elections for the Senate, Chamber of Deputies and the President of Romania. The law was passed so that Romanian citizens in diaspora could

[48] For more information: Romanian Legislative portal: http://legislatie.just.ro/Public/DetaliiDocument/46899, (ORDONANŢA DE URGENŢĂ nr. 93 din 9 octombrie 2003 (*actualizată*)), last accessed: November 2020,

[49] For more information: Romanian Legislative portal: http://legislatie.just.ro/Public/DetaliiDocument/173139, (LEGE nr. 288 din 19 noiembrie 2015), last accessed: November 2020

exercise their rights to vote in a more reasonable manner without having to stand in line for several hours at the precinct station.

An actual legislative proposal was submitted in Parliament in 2015[50] by 7 deputies and senators (PNL, PP-DD and independents) regarding the organization and implementation of electronic voting. Although the legislative proposal was very comprehensive and included details such as an electronic voters' register, the responsible institution, the budgetary framework, and the implementation procedure, it was rejected in the Senate, the first chamber, by 95 votes against and just 2 for it with 2 abstentions. The proposal is still in the second chamber, the decisive one, where it has received ongoing negative feedback from the government as recently as this year.

There is another aspect that does not refer to electronic voting per se but is relevant to our discussion: In 2016, the SIMPV[51] Informatic System was introduced to monitor turnout and illegal voting in local and parliamentary elections. What is important about this system is the fact that before it became functional in voting precincts it had been piloted since 2011 in several local elections and had been improved from one electoral cycle to the next evolving from identity card scanners to scanning with tablets at the precinct stations.

CURRENT SITUATION

A declaration[52] from the President of the Permanent Electoral Authority in Romania states that: "The Authority is involved in an e-government project. Although all the European States had the obligation to introduce the electronic vote and Internet voting, we have today only one state that actually has it. We have a plan for 2024, the year when all levels of elections will be held during the same year—local, euro-parliamentary, parliamentary and president—to implement this voting system.

Two legislative proposals are currently in Parliament that refer to electronic voting.

- **One proposal initiated by senators and deputies from USR party.** [53]
This legislation proposes an experimental phase that will take place during three elections in constituencies that will be selected randomly. The proposal also stipulates that electronic voting software should be open source so that audits and analysis can be carried out by independent institutions. Unlike previous proposals, this one suggests the use of qualified or advanced digital certificates, not just a user name and a password. The elector has to make an

[50] For more information: Senate Chamber legislative portal: https://www.senat.ro/legis/lista.aspx?nr_cls=L418&an_cls=2015 last accessed: November 2020

[51] "Sistemul anti-fraudă la vot, introdus la alegerile de duminică", Digi24, 2016 https://www.digi24.ro/special/dosare/alegeri-locale-2016/sistemul-anti-frauda-la-vot-introdus-la-alegerile-de-duminica-524205,

[52] Mihai Gongoroi, "Presedintele AEP a spus in ce an va fi introdus in Romania votul pe Internet", Mediafax, 2019 https://www.mediafax.ro/social/presedintele-aep-a-spus-in-ce-an-va-fi-introdus-in-romania-votul-pe-internet-18671044, 2019

[53] For more information: Senate Chamber legislative portal: https://www.senat.ro/legis/lista.aspx?nr_cls=L244&an_cls=2019, (L244/2019 - Propunere legislativă privind organizarea şi desfăşurarea votului electronic la distanţă), last accessed: November 2020

official request that can be done online, but receiving a digital certificate has to be in person.

One subject that the proposal tries to address is the secrecy of the vote, as it is very often one of the major arguments against electronic voting. However, the initiative refers only to the anonymity of the vote in relation to voters, meaning the system should never allow a vote to be associated with the person who cast it.

The electoral process should start six days before the date of the election and end one day before it. During the early voting period, the voter can vote several times, but only his/her last vote will be taken into consideration. Vote counting should be realized through a different information system than voting casting and it shouldn't be connected to a network or to the Internet.

This proposal was adopted by the Senate in September 2019 and progressed to the Chamber of Deputies that will decide. The proposal received negative feedback from the government in July 2020.

- **Another proposal initiated by senators and deputies from the PNL party.[54]**

This proposal is clearly less complete as a stand-alone document than the one proposed by USR and refers to the modification of the 288/2015 law regarding correspondence voting. Basically, it introduces a model for electronic voting compared with voting by correspondence and adds a paragraph about a registry for electronic voting.

In March 2019 the legislative proposal was rejected by the Senate with 63 votes against and 23 for and then progressed to the Chamber of deputies. The proposal has so far received favourable reports from the Committee for Romanian Communities outside the Country, from the Committee for Human Rights, Cults and National Minority Problems and negative reports from the Committee for Equality of Opportunities for Women and Men and the Committee for Information Technology and Communications.

The proposal was sent for report in June 2019 to the Special Committee of the Chamber of Deputies and Senate for the elaboration, modification and completion of legislative proposals regarding elections.

[54] For more information: Chamber of Deputies legislative portal: http://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?cam=2&idp=17381, (Pl-x nr. 146/2019), last accessed: November 2020

Until now, the opinion of the government about all the proposals has always been against electronic voting. It is helpful to see what the arguments in their negative reports are if we want to understand what challenges have to be overcome so that this objective can be achieved:

- The secrecy of the vote which is guaranteed by the constitution might require any proposal in this regard to be rejected for reasons of unconstitutionality. The secrecy of the vote refers to two aspects: one is the anonymity of the vote—ensuring the fact that the vote cast is not connected to the identity of the voter—which can be handled and solved through the right technology. The second, which is still a challenge, is the fact that the voter can cast his/her vote in secrecy. In past years, several fraudulent systems were used for electoral bribing or intimidation and were resolved through the presence of observers from the concurrent parties and independent observers in the precincts. With online voting, none can give any insurance that the voters—especially older ones and those from vulnerable groups—will not be influenced by someone telling them how to vote. In one of its negative comments on legislative proposals regarding the introduction of electronic voting, the government quotes the Code of Good Practices in Electoral Matters adopted by the Venice Commission which stipulates that "electronic voting methods must be secure and reliable"[55].
- The fact that any legislative proposal must include not only the motives of the initiators but also a rather comprehensive impact study stipulating the technical hardware and human resources needed, and the budgetary impact.
- The fact that such a legislative proposal should not be adopted without several trials before it is approved so that possible problems can detected and solved.
- The fact that such a voting system introduced only for the diaspora might discriminate against the rest of Romanian citizens who could also benefit from this procedure plus the fact that an IP control system would be needed to certify that the person voting is actually outside the country and not in the country.

[55] European Commission for Democracy Through Law (Venice Commission), Code of Good Practice in Electoral Matters, Strasbourg, 2002, Paragraph 43, page 22

CONCLUSIONS:

- Romanian citizens have a certain degree of distrust in electoral processes, although they have visibly improved over time. However, tampering with the status quo will trigger many doubts both from the political parties as well as from the average citizen who votes.
- There is no doubt that decision makers from all parties understand the importance of the use of electronic voting, but they are also sceptical about the security of the system, possible flaws, hacking, etc.
- In order to move forward, the example of the SIMPV Informatic System to monitor turnout and illegal voting could be replicated. It is obvious now that no government, regardless of the political party, will adopt such a system without testing it before and without convincing the public that there is no risk of electoral fraud.

CONSIDERATIONS FOR THE INTRODUCTION OF INTERNET VOTING IN THE REPUBLIC OF MOLDOVA

By Alexandru Balmoș
Head of IT Department of Central Election Committee of the Republic of Moldova

On 15 May 2008, the Parliament of the Republic of Moldova adopted Law No. 101 on the Concept of the State Automated Information System Elections (SAISE)[56]. SAISE's long-term goal is to fully automate elections in Moldova. Electronic voting implies using the Central Electoral Commission's (CEC) information portal and will give the voter the opportunity to vote from anywhere in the world, either through electronic voting terminals (for example, using an electronic pen, scanner or other electronic input device) and/or using the Internet using identification devices that can read electronic documents.

Electronic voting can be exercised using digital signature mechanisms if the voter has a private key for digital signatures and a valid public key certificate issued in accordance with the legislation regarding digital signatures, both being compatible with the hardware and software of SAISE. In 2016, a feasibility study on Internet voting was conducted for the CEC in cooperation with the United Nations Development Program (UNDP) in Moldova[57]. In conclusion, Moldova has all the necessary prerequisites for the introduction of an Internet voting system in the near future including a well-developed Internet infrastructure; a high degree of coverage by mobile networks; an adequate education level among the population in information and communication technologies; reliable electoral lists (State Register of Voters); and polling stations equipped with computers connected to the Internet that are permanently online and communicate with SAISE.

[56] For more information: Official Monitor Lex Justice http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=328369, (LEGE Nr. 101 din 15.05.2008), last accessed: November 2020

[57] For more information: Feasability Study on Internet voting for CEC Moldova https://www.md.undp.org/content/moldova/en/home/library/effective_governance/feasibility-study-on-internet-voting-for-the-central-electoral-c.html last accessed: November 2020

CURRENT SITUATION

First of all, it is necessary to adopt a lasting political decision on the broad acceptance of this system by all relevant political parties. This acceptance is essential because the introduction of Internet voting and the authorization of all the necessary regulations will inevitably involve significant costs in terms of funds, time, and human resources; the return on this investment is a long-term one.

The Electoral Code of the Republic of Moldova does not include specific provisions regulating the concept of Internet voting—relevant policies, rules, procedures and operating criteria—or the requirements for managing an Internet voting system. In order to create an appropriate legal framework for the implementation of Internet voting, the Electoral Code is to be modified by introducing Internet voting concepts, vote verification and cancellation rules, principles for ensuring the secrecy of voting, voter identification aspects, information systems that establish the framework for the operation of Internet voting, security and audit requirements, and other elements common to Internet voting.

Following the analysis of the legal framework, the demographic situation and the level of development of information and communication technologies carried out during the feasibility study, it was concluded that it is feasible to create an Internet Voting Information System (IVIS), owned and managed by CEC as a module of SAISE. IVIS is to be used by the CEC as an alternative voting channel, via the Internet, in national elections and referendums held in the Republic of Moldova as well as in consultations with citizens and private elections. The basic function of IVIS will be to provide Internet voting services with the capacity to provide such services to the government (ministries, public authorities, etc.), mayoralties, city councils, NGOs and private entities. Thus, for the large-scale implementation of the IVIS module, implementing an IVIS pilot project was proposed.

According to the development plan and the roadmap for introducing I-voting, a technical concept was developed in 2019 in the context of developing the IT subsystem for remote electronic voting. Thus, SAISE e-voting is defined as a functional component of the SAISE which in turn is part of the state information resources that aims to automate the preparation, assistance and analysis of election results in Moldova.

SIS e-voting can be implemented due to the e-Government Agency of the Republic of Moldova using the MConnect[58] interoperability platform for data exchange with third-party IT systems, MCloud (MPass, MSign, MNotify, MLog)[59] platform services and the Open Data Portal for the implementation of basic functionalities and publication of public information produced in the process of remote electronic voting. The holder of the IT solution is the CEC which will provide the technical infrastructure that will host SIS e-voting. The possibility of hosting some SIS e-voting components outside the CEC data center in the future is not excluded. A solution in this regard could be the common government platform MCloud.

The design, development, implementation and operation of SIS e-voting requires the involvement of several government institutions such as the Electronic Government Agency, the Information Technology and Cyber Security Service and public authorities interested in implementing remote electronic voting. The Information Technology and Cyber Security Service,[60] as the administrator of the single public key infrastructure (Single Certification Centre of the Government), plays an important role in the use and provision of digital signature mechanisms. The term of validity of the user's public key certificate is established by the certification service provider, which at the moment cannot exceed more than 1 year. However, as the number of active users of the electronic signature service has increased, extending the validity of the public key certificate from 1 year to 2 years was approved[61] with the prospect of extending it to 5 years. The accessibility of digital signature mechanisms will have a significant effect on IVIS implementation[62].

Despite the fact that the number of holders of personal authentication electronic certificates is still quite small, their popularity is growing rapidly and is expected to grow continuously[63] as the government plans to provide more and more electronic services.

In its 2020–2023 Strategic Plan and as the continuation of events and actions already carried out,[64] the CEC has approved the objective of developing an Internet voting system in the future. Thus, the commission is tasked with drafting terms of reference for the implementation of the module and the introduction of IVIS by 2022. The preparation of the terms of reference, including all the stages of identifying and selecting the entities that are going to be involved in the implementation, will add up to 12 months.

[58] For more information: E-Governance Agency of the Republic of Moldova https://egov.md/en/projects/mconnect, last accessed: November 2020

[59] For more information: E-Governance Agency of the Republic of Moldova https://egov.md/en/projects/m-cloud, https://egov.md/en/projects/m-pass, last accessed: November 2020

[60] For more information: Information Technologies and Cyber Security Service ot the Republic of Moldova https://stisc.gov.md/, last accessed: November 2020

[61] For more information: STISC Moldova https://stisc.gov.md/ro/termenul-de-valabilitate-al-certificatului-cheii-publice-s-extins-de-la-1-la-2-ani, last accessed: November 2020

[62] For more information: STISC Moldova https://semnatura.md/, https://www.legis.md/cautare/getResults?doc_id=112497&lang=ro, (Republica Moldova, PARLAMENTUL, LEGE Nr. 91 din 27-06-2014), last accessed: November 2020

[63] For more information: State Chancellery of the Republic of Moldova, Cotidianul Newspaper, https://cancelaria.gov.md/sites/default/files/air_pl_identificarea_electronica.pdf, last accessed: November 2020

[64] For more information: Central Election Committee of the Republic of Moldova, https://a.cec.md/storage/ckfinder/files/RVC%20CE/Anexa_Plan%20Strategic_CEC.pdf, last accessed: November 2020

The CEC will develop the IVIS technical task as a component part of SAISE (module). It would therefore be timely now to establish a permanent steering committee to coordinate the preparation, creation, introduction and implementation of IVIS which would include CEC members, representatives of the CEC administration, of the Ministry of Information Technology and Communications, of the Information Technology and Cyber Security Service, of the e-Government Centre, of the Public Services Agency[65], of development partners (e.g. UNDP) and of other relevant institutions. The Action Plan for IVIS development will include the following:

- **Preparation of the technical specifications, an operating regulation and the procurement plan for IVIS implementation, as well as a plan for testing the performance, security and functionality of the pilot and its implementation;**
- **Coordination of harmonization of the electoral legislation for purposes of official implementation of the IVIS;**
- **Coordination and submission of proposals for draft CEC decisions on the creation, introduction and implementation of the IVIS;**
- **Creation of the IVIS regulation: technical regulatory documents, IVIS security regulatory documents, technical and procedural instructions;**
- **Preparation/coordination of the technical documentation related to IVIS and its processes.**

One of the most important aspects of IVIS implementation is its funding. At present, funds from the state budget have been allocated for this project; however, for these resources to be received, it is necessary to adjust the regulatory framework and carry out all the steps described above. The IVIS pilot stage can be carried out at the next national election organized by the CEC under regular procedures. The pilot version should provide technical, functional and security solutions as if legally binding elections had been held, except for the legal validity of the results. This is an important requirement both for testing the security and reliability of the Internet voting system and for gathering valuable opinions from experts and civil society. Therefore, the CEC will coordinate the implementation of the plan for testing performance, security and functionality with the subsequent preparation of the test reports.

[65] For more information: Public Services Agency, Moldova http://www.asp.gov.md/en, last accessed: November 2020

After the pilot project, the participants will provide their feedback and a report will be drawn up and submitted to the CEC/IVIS permanent steering committee so that any knowledge gained in the pilot project will be used in the official implementation of the IVIS.

The implementation of the IVIS is absolutely necessary for the Republic of Moldova because Moldova is a state where the phenomena of migration and voter absenteeism are very pronounced. As a result, the participation rate of voters steadily decreases. Given the advanced level of implementation of e-government initiatives in the Republic of Moldova, there are solid prerequisites from a technological point of view to implement a remote electronic voting system that corresponds to modern requirements. This would significantly increase the involvement of the diaspora and young people in electoral processes.

At the same time, in the long run, with the popularization of Internet voting, the e-service could be used by state and municipal institutions to organize consultations with citizens, organize internal elections by political parties, NGOs, academic communities and other institutions that need electronic solutions for organizing elections or other decision-making processes in a secure and transparent way.

Given the COVID-19 infection-related pandemic situation and an analysis of the organization of the presidential election that took place in the Republic of Moldova on 1 November 2020, there was a need for a system that would allow remote voting, primarily to ensure the safety of the voters and election officials as well as to reduce the cost of purchasing protective equipment for electoral bodies.

Future perspective

Internet voting is not only an alternative to traditional or postal voting; it can become a reality for a society dominated by technological solutions and the needs of our times when the capabilities of millions of citizens and diaspora members to get to polling stations to exercise their right to vote are limited. Of course, the implementation of Internet voting involves a range of political, social, financial and technological challenges, but all of these can be solved with sufficient political will and cooperation between public and private institutions and citizens.

Several technical defining elements are needed to develop an Internet voting system:

- a secure and credible system for citizens' digital authentication;
- secure data interoperability and a circulation system among different state registers;
- a robust and reliable infrastructure;
- a legal framework that tackles these challenges among which are personal data protection and the implementation of the once-only principle and of ballot secrecy.

Internet voting systems are reliable and work only when there is sufficient credibility in entities organizing and implementing these systems, both from a decisional and technological point of view. A digitally developed society that broadly uses other e-governing solutions will more easily accept and implement I-voting.

Nonetheless, the main promoter and at the same time the main barrier in implementing I-voting is the presence or lack of political will, by either assuming or failing to assume responsibility for implementing this complex process. Politicians often bring a range of arguments for not starting a wide debate on how to solve these challenges, even if there is enough expertise and good practice in the field. One example is the argument that votes can be influenced or even bought, despite the fact that an Internet voting system can be set up for multiple voting with only the last vote counting. Moreover, a traditional vote at the polling station on election day will nullify all previous online votes. Another argument refers to the impossibility to check a vote after casting it online. In Estonia, there is already the possibility to check on a vote via a QR code. There has not been not a single hacked I-vote there since I-voting was first implemented in 2005, which proves the safety of these systems, and online security systems have gradually become more complex and secure over time.

Developing digital skills among citizens through various programs and setting digital education as a core priority for all levels of education is a key element. The entities that plan for and implement the digital transformation process and implicitly, I-voting, must be open for discussions about the potential challenges and issues, because society has this right. This is the only way credible I-voting systems can be built and used on a large scale. There will never be a perfect I-voting system just as there is no perfect traditional or postal voting, but every election will provide lessons and solutions for further improvement by applying the principles listed.

Internet voting has to be one voting option among traditional ones, and citizens should have the possibility to choose the most convenient way to express their votes. A quick metamorphosis from traditional to online voting without considering potential risks can be dangerous, counterproductive and can compromise the idea of implementing I-voting in the future. In contrast, gradual implementation is recommended, starting with less significant elections, local referendums or consultations so that people can understand the functionality and benefits of this voting option. It is not necessary to copy a solution entirely. Various elements can be borrowed from different existing systems and adjusted to the best options required for the country.

Time, resources and efforts by society members will be needed to understand, develop and implement this option, as well as the establishment of a broad coalition of political, civil society, academic community, community, and citizen stakeholders. However, we are sure that any democratic state will choose this voting option for elections sooner or later. The earlier this process starts, the quicker a reliable, efficient and safe system with enormous benefits for all will be created.

Bibliography:

1. **Lang, M. The Athenian Citizen, Democracy in the Athenian Agora. 2004**
   http://www.agathe.gr/democracy/practice_of_ostracism.html

2. **Jay S.Coggins and C.Fererico Perali, Public Choice, 1998,**
   https://www.apec.umn.edu/sites/apec.umn.edu/files/64-majority-rule-in-ducal-venice.pdf

3. **Htet Ne OO , A Survey of Different Electronic Voting Systems, Htet Ne OO,**
   2014 https://www.researchgate.net/publication/321431416_A_Survey_of_Different_Electronic_Voting_Systems

4. **Martin Russel, Ionel Zamfir, European Parliamentary Research Service, 2018**
   https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf

5. **Drew Springall and Team, Security Analysis of the Estonian Internet Voting System,**
   2014https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

6. **Jasper Bakker, Computer Weekly, 2017**
   https://www.computerweekly.com/news/450424978/Dutch-e-voting-is-waiting-for-an-opportunity

7. **Kristjan Vassil, Does Internet Voting Bias Election Results? Evidence from Estonia, 2014**
   https://www.ut.ee/kristjan.vassil/wp-content/uploads/Bias_report.pdf

8. **Feasability Study on Internet voting for CEC Moldova**
   https://www.md.undp.org/content/moldova/en/home/library/effective_governance/feasibility-study-on-internet-voting-for-the-central-electoral-c.html

9. **Meredith Applegate, Thomas Chanussot, Vladlen Basysty. Considerations on Internet Voting: An Overview for Electoral Decision-Makers, 2020**
   https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

FRIEDRICH NAUMANN
FOUNDATION For Freedom.

Romania and Moldova