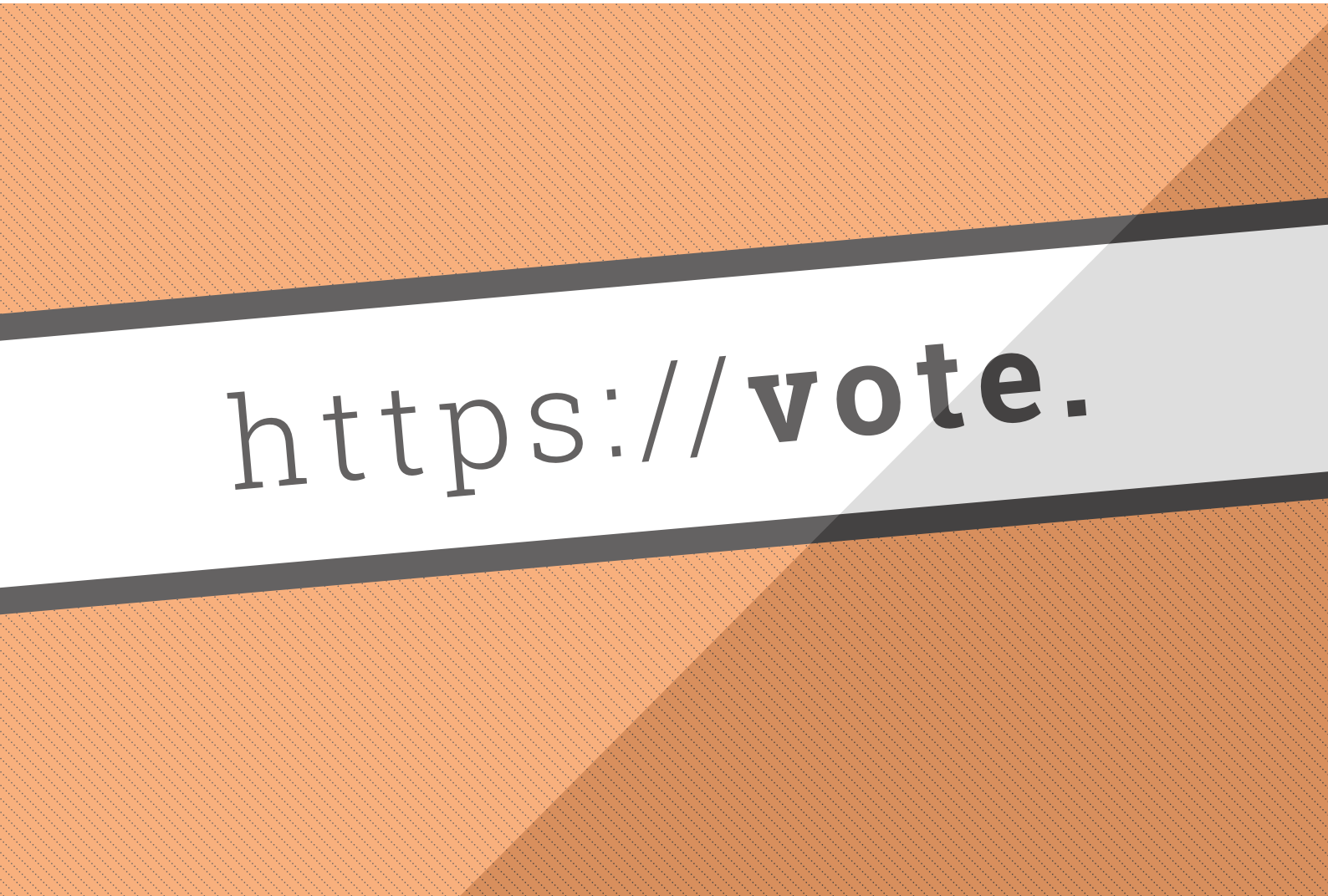
EXPERT FORUM

PAPER VS INTERNET: IS ELECTRONIC VOTING A SOLUTION FOR ROMANIA?



AUTHOR

Septimius Pârvu

Project financed by the EEA grants 2009–2014, through the NGO Fund in Romania.

Fundația pentru
Dezvoltarea
Societății
Civile

www.expertforum.ro

PAPER VS INTERNET:
IS ELECTRONIC VOTING
A SOLUTION FOR ROMANIA?

CONTENTS

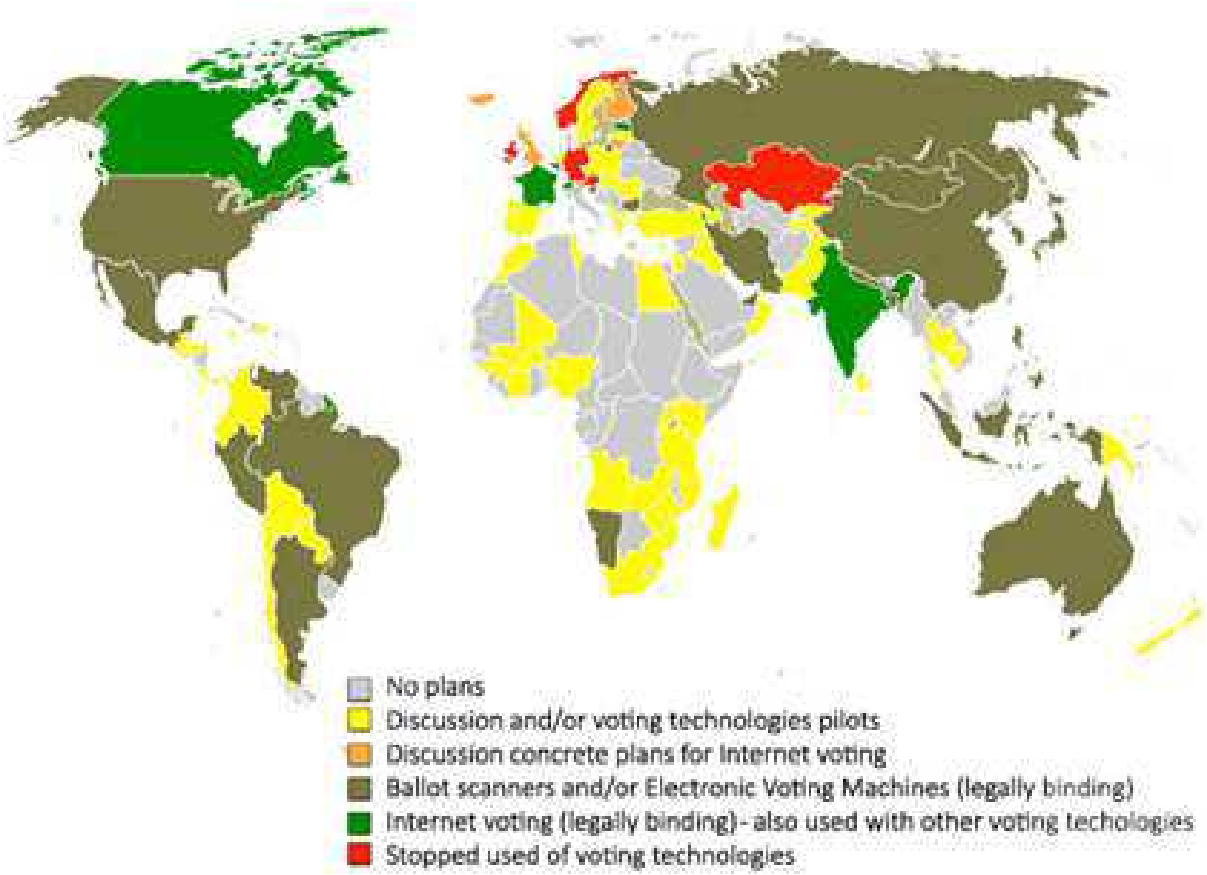
Countries such as Estonia or France managed to implement internet voting, even though the system was criticized. Other countries, such as the Republic of Moldova are making important steps for introducing this voting method soon. Romania has been avoiding for many years to make a decision that could ease voting in diaspora. In this report, we are presenting the Baltic experience, especially the Estonian one regarding internet voting. Estonia is the only country which applies internet voting for every type of election and has proven until now one of the most successful examples. Nevertheless, Estonia was also criticized regarding security issues or possible frauds.

Thus, we analyse the way the Estonian vote, why it is a successful example and why other countries failed to use technology in expressing electoral options. We included in the report conclusions of meetings with electoral experts, members of electoral commissions or academia, as well as the conclusions of our own observation mission in Estonia, Latvia and Finland.

In Romania the discussion is stalling, it lacks arguments and is not open to the public, with no consultations with the citizens. We are talking about fear of electoral fraud, system manipulation possibilities or citizens' limited technological abilities. But we are not talking about objectives, clear steps, taking political responsibility over a project that has proven controversial in every country in which it was tested.

What are the conditions for Romania to implement electronic voting through internet and what steps should the politicians and authorities make?

Electronic voting is one of the most controversial methods of expression electoral options. If some countries like Estonia consider that it is a well-functioning system and it is suitable for its citizens, others such as Netherlands or Germany consider using machines or online technologies to vote an unsafe method, arguing about constitutional aspects or generating uncertainty at expressing and quantifying electronic votes. Norway gave up testing due to security hazards. What is certain is that there are plenty of countries which were tempted to adopt electronic voting (internet voting or machine operated voting) and a significant number of countries consider that this is the future.



World map of electronic voting. Source: http://www.e-voting.cc/

Politicians and the society, including in Romania, are permanently debating subjects such as vote safety, paper vote vs invisible vote or the fact that the electronic vote cannot be observed and understood by everyone. There is also the less visible reason of political parties' fear of undertaking a significant risk with an electronic voting system, whose effects could alter election results. The discussions are mostly populist and groundless. Rarely there are mentions of the system's architecture, documents used for authentication, but also about the positive side of electoral and constitutional rights. It is true that in many of the countries that today apply electronic voting in any manner or gave it up there were discussions concerning the constitutional equality-wise of the paper vote with the electronic vote, but also about the secrecy of exercising electoral rights. Opinions are divided and are subject to each state's constitutional vision.

One of the countries that has significantly advanced regarding electronic voting through internet and that managed to implement a fully functional system is Estonia. Practically, in 2015 it is the only country in the world with electronic voting through internet, for any type of elections, for over ten

years. Officially, there are no major scandals, vote cancellations or electoral fraud; but that does not mean there are no criticisms and contestations. On the other hand, neighbouring countries such as Finland, Latvia or Lithuania are struggling or have already failed at voting electronically, either with voting machines or on-line.

Electronic voting in Estonia is considered a great success in the same time, but some raise legitimate questions. If for Estonian authorities, system vulnerabilities are disregarded or could be solved, for some academia and international authorities there are problems that should lead even to eliminating electronic voting from Estonian legislation and practice.

Nevertheless, we must look carefully at the lessons that can be learnt from the Estonian experience and from the criticism brought by experts to the Baltic model. The following conclusions are the result of a documenting visit in Estonia, Finland and Latvia whose purpose was the identification of pros and cons of electronic voting and of good practices that can be adopted. The visit took place between 27th February and 6th March in Tallinn, Helsinki and Riga and included meetings with electoral experts, members of national electoral commissions, IT specialists, academia and also with representatives of international organization whose role is to observe elections. We took part to a visit at the Romanian Embassy for Finland and Estonia. The topic of the meeting was the organization of the voting process abroad and Romanians' situation in the two countries. On the 1st March we observed the parliamentary elections in Estonia in five polling sections and assisted in the opening and counting of electronic votes.

The purpose of this report is not to offer IT solutions, but more to put on the public agenda, with arguments, the opportunity of introducing internet voting in Romania.

WHAT IS THE STORY OF ELECTRONIC VOTING[1] IN ESTONIA

The first steps for introducing electronic voting took place in 2002. It was used for the first time extensively in 2005 for the local elections. Before completely using all the components of the process there were multiple partial tests. In 2015, ten years after the first usage, Estonia is the first and only country to be able to brag about using electronic voting through internet for all types of elections, inside or outside the country.

	Local Elections 2005	**Parliamentary Elections 2007**	**European Parliament Elections 2009**	**Local Elections 2009**	**Parliamentary Elections 2011**	**Local Elections 2013**	**European Parliament Elections 2014**	**Parliamentary Elections 2015**
Eligible voters	1.059.292	897.243	909.628	1.094.317	913.346	1.086.935	902.873	899.793
Participating voters (voters turned out)	502.504	555.463	399.181	662.813	580.264	630.050	329.766	577.910
Voter turnout	47,4%	61,9%	43,9%	60,6%	63,5%	58,0%	36,5%	64,2%
I-voters	9.317	30.275	58.669	104.413	140.846	133.808	103.151	176.491
I-votes counted	9.287	30.243	58.614	104.313	140.764	133.662	103.105	176.329
I-votes cancelled (replaced with paper ballot)	30	32	55	100	82	146	46	162
I-votes invalid (not valid due to a nonstandard of vote)	n.a.	n.a.	n.a.	n.a.	n.a.**	1	n.a.	1
Multiple I-votes (replaced with I-vote)	364	789	910	2.373	4.384	3.045	2.019	4.593
I-voters among eligible voters	0,9%	3,4%	6,5%	9,5%	15,4%	12,3%	11,4%	19,6%
I-voters among participating voters	1,9%	5,5%	14,7%	15,8%	24,3%	21,2%	31,3%	30,5%
I-votes among advance votes	7,2%	17,6%	45,4%	44%	56,4%	50,5%	59,2%	59,6%
I-votes cast abroad among I-votes (based on IP-address)*	n.a.	2% 51 states	3% 66 states	2,8% 82 states	3,9% 105 states	4,2% 105 states	4,69% 98 states	5,71% 116 states
I-voting periood	3 days	3 days	7 days	7 days	7 days	7 days	7 days	7 days
I-voters using mobile-ID	n.a.	n.a.	n.a.	n.a.	2.690	11.753	11.609	22.084

1. We are referring to electronic voting through internet

	Local Elections 2005	Parliamentary Elections 2007	European Parliament Elections 2009	Local Elections 2009	Parliamentary Elections 2011	Local Elections 2013	European Parliament Elections 2014	Parliamentary Elections 2015
I-voters using mobile-ID among I-voters	n.a.	n.a.	n.a.	n.a.	n.a.**	1	n.a.	1
Share of I-votes that were verified by the voter	n.a.	n.a.	n.a.	n.a.	n.a.	3,4%	4,0%	4,3%

** in Local Elections, voters permanently residing abroad are not eligible for voting*

*** one invalid vote is depicted among cancelled votes*

The system was developed in three steps. First there was a general idea about what is desired, a technical solution (2002). In the second step, in 2003-2004, the basic system was developed, through consultations with the civil society and academia. There were two main proposals regarding the architecture of the system. At the third checkpoint, in 2005, a more complex version of the law was elaborated. During all this time, there generally was a political consensus, without which no negotiations could have been possible. The system cost 2 million euros, to which approximately 50,000 – 60,000 Euro are added for its update before the elections.

The first important lesson is that without a solid political consensus and clear objectives, electronic voting stands no chance. The experience shows that in other countries this attempt failed because there was no common ground among parties or there was strong criticism from third parties. Lithuania and Latvia are two visible examples in this sense. The Latvian case also proves that a public consultation is needed, as the impact on the final result can be decisive. In Latvia there was a strong opposition against the system from academia and IT areas (less those who would have developed the system's software). This fact led to the end of any discussion about implementing electronic voting for unsafety reasons.

Neither the legislative path of the Estonian electronic voting system was a smooth one, as some parties constantly criticized the system's vulnerabilities. Eesti Keskerakond (Centre party) – whose electorate mostly consists of retirees and Russians – is the system's main critic, even though during the 2015 elections it encouraged voters to use electronic means of voting. There were more recurrent subjects brought by parties to the public agenda. Some politicians considered that these efforts should not be made; who does not want to go to the voting station should not vote. Also, they feared that the electronic vote could bring new people to vote, who could change the scale. Finally, the electronic vote cannot be supervised and comprehended, is unsafe, thus it is not legitimate. However, practice does not show that participation grew too much due to electronic voting; it also did not visibly affect the political balance. The Centre party received few electronic votes due to its profile and voters who generally reject the concept. The Reform Party, who initiated the project, did not necessarily get the most electronic votes.

Estonia's more likely conservative president, Arnold Rüütel, contested the law before the 2005 local elections at the Supreme Court, motivating that the possibility to change the vote favours on-line voters. The Court considered that there is no discrimination, as the electronic voting and also the paper ballot create the same judicial effects. Furthermore, all citizens have access to electronic voting, so there are no discriminatory barriers.

A very important reality that conditions the way electronic voting is discussed and functions is the trust the stakeholders have in the system, in the electoral authorities and in political parties. In Estonia, citizens have faith in the electoral process. From discussions with interlocutors the outcome was that there are no major electoral frauds or complaints, but rather minor incidents, which do not visibly affect the election process. This fact was also noticed during the day of the vote[2]: citizens respect the rules and there are no major incidents who could lay (significant) doubts over election results.

2. We observed the elections in five polling stations in Tallin and outside of the capital, including a polling station organized in a supermarket

HOW DOES THE ELECTRONIC VOTE WORK?

First of all, electronic voting must be used together with other methods: paper ballot, by post, in advance in the voting section (2 types) or on ships.

First, in organising electronic voting multiple institutions are involved:

- National Electoral commission
- Electoral Commission for Electronic Voting – composed of 7 members at most, named by the National Electoral Commission; has the role of organizing and managing electronic voting, checking the votes
- Electoral administration: constituency electoral bureaux and those of voting sections
- Riigi Infosusteemi Amet (RIA) – public institutions with a role in managing IT infrastructure
- Sertifitseerimiskeskus AS – private company, the only digital certification supplier
- Cybernetica AS – the company who developed the system
- KMPG Baltics AS - the auditor of the electronic voting system. Checks the security of the process from the perspective of voters lists, votes transfer between the system's components or the counting process of votes

Nothing would be happening in Estonia without the **identification documents with electronic chip**. Estonia started to build a centralized system at the end of the '90s, which gathers information about citizens, such as education, health, etc. This information is held by the public authorities decentralized, but the databases communicate through a unique portal, www.eesti.ee. The portal can be accessed by public authorities, citizens and companies. The Ministry of Finance is the one who manages the architecture of the system. Some voices consider that centralizing the data is not auspicious, especially in the case of an IT attack; authorities and citizens see the integrated system as a very useful mechanism. A similar framework also exists in Norway.

Every citizen (and under some conditions the residents) receives an identity document with a chip (www.id.ee), which can be used to access various services offered by public authorities, but also by banks, for example and two PINs: one used to authenticate in order to use various services, including electoral ones and the second PIN, which is actually a digital signature.

Source: https://www.valimised.ee

Two email addresses are issued along with the card, one with the person's name and the ending @eesti.ro. The second address corresponds with the unique registration number every Estonian is issued and has the same ending.

In order to be able to vote, citizens can use the ID or a **Mobiil-ID** card, which can also be used to access public services. A third way – more recent – is with the help of a **SIM card** issued by one's mobile phone provider, but which must be registered at the Police and Border Police.

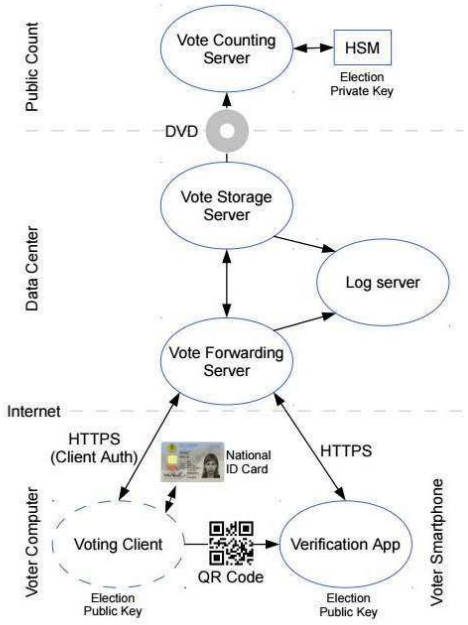
The electronic voting takes place in advance. The voters can change their vote as many times as they wish during this time, but they cannot vote during the election day (initially the law allowed for this possibility). The last expressed vote is the valid one: electronic, if the voter voted only by internet, or the paper ballot, if the voter changed his/her vote in the polling station. The same principle is also applied in the electronic voting system in Norway. The Estonian mechanism allows the citizens to change their vote in the situation in which there was pressure upon them, being considered a method of applying vote secrecy.

Alegerile parlamentare 2015

<table>
<tr><td>Th
19.02.</td><td>Fr
20.02.</td><td>Sa
21.02.</td><td>Su
22.02</td><td>Mo
23.02.</td><td>Tu
24.02.</td><td>We
25.02.</td><td>Th
26.02</td><td>Fr
27.02</td><td>Sa
28.02.</td><td>Su
01.03.2015</td></tr>
<tr><td colspan="7">ADVANCE VOTING</td><td colspan="3" rowspan="3">NO VOTING</td><td>ELECTION DAY</td></tr>
<tr><td colspan="4">Advance voting in county towns
12 a.m. – 8 p.m.</td><td colspan="3">Voting at voting districts
12 a.m. – 8 p.m.</td><td>Voting at voting districts
9 a.m.– 8 p.m.</td></tr>
<tr><td colspan="7">E-voting
valimised.ee
9 a.m. ... ... - 6 p.m.</td><td>Voting at home</td></tr>
</table>

+ **Voting abroad** (by post, at foreign missions, via Internet)

The voting procedure is done through a downloadable application from the webpage www.valimised.ee. This was used for the first time in 2011; prior to this the electoral authorities were using a Java application which was running from the browser. The head of the Electoral Commission for electronic voting believes this system is more secure and can also ensure the scan of the user's computer, thus eliminating the possibility of malware.



I-voting system overview — Major components of the system, and how information flows among them
Source: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

For the registration and centralization of the votes there are three servers[3]:

- The forwarding server: authentication, transfer of the list of candidates to the voters, reception of the votes (not anonymised)
- The storage server: centralizes the encrypted votes until the end of the voting period
- The counting server (*offline*): receives the transferred votes on a CD/DVD, anonymised and counts them

The voting procedure is based on the principle of the double envelope. Initially, the voter expresses the vote which is then transmitted to the server in an envelope which contains the actual vote and the identification data. Before the counting of the votes, the anonymised option is moved in another envelope that is practically counted.

3. Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman, Security Analysis of the Estonian Internet Voting System, *https://jhalderm.com/pub/papers/ivoting-ccs14.pdf*

VOTE VERIFICATION AND ELECTION OBSERVATION[4]

One of the most important steps of the process is the vote verification. In the Estonian system, the voter can check using a QR code if his/her vote was registered and if it was correctly accounted for. If at first the system only indicated if the vote was registered, recently any voter can check by using a phone application and by scanning a QR code generated at the end of the voting process if their option was correctly registered, by showing it for 30 seconds in the application. The 30 seconds limit is according to the electoral authorities a safety mechanism against checking by third parties of the voted option[5].

Another verification system is the Norwegian one in which the voter receives by post a paper card with unique control keys for every person, which correspond to each party[6]. At the end of the voting procedure, the voter receives a four digit code by SMS which should correspond to the initial options. This system was introduced by electoral authorities also as a control mechanism of system attacks. For example, a system manipulation would get detected if 1% of voters (in the case of elections where 40,000 votes were registered) would check; in this situation the chance of detecting manipulation is of 90%.

The Estonian system also includes other mechanisms of monitoring the process. Firstly, any citizen can observe the e-ballot opening and counting procedures. At the parliamentary elections of 2015, the counting took place between 6 PM and 8 PM at the Parliament building. The authorities denied access in the room with mobile phones and photo cameras, considering that at the latest elections the results were shared earlier in the public. As a rule, any citizen can observe the elections without restrictive accreditation conditions; practically, anyone can go in the voting section without prior registration.

In order to allow the verification of the source code, the authorities published a big part of it on the webpage https://github.com/vvk-ehk/evalimine. There was criticism from some IT technicians and experts because the full code was not published; the authorities consider that the publication of the entire code would be an element of vulnerability.

4. For more examples related to vote integrity and verifiability see *http://www.e-voting.cc/en/portfolio-item/proceedings-2012/*

5. More about the verification procedure here: *http://vvk.ee/public/Verification_of_I-Votes.pdf*

6. Ida Sofie, Gebhardt Stenerud and Christian Bull. When *Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting*, *http://www.e-voting.cc/wp-content/uploads/downloads/2012/07/21-33_Stenerud-Bull_Norway.pdf*

CRITICISM BROUGHT TO THE ELECTRONIC VOTE

The most virulent report published[7] against the system is considered by the Estonian authorities with mistrust. The report written by international IT experts concludes shortly that the Estonian electronic voting system has too many vulnerabilities and must therefore be cancelled. There are voices which say that the report is paid by the centre pro-Russian Party, one of the most visible critics of the electronic vote.

The authors criticize the quality of the human resources on one hand and on the other they warn about possible ways of infiltrating the system and changing the result of the vote. Among the reported vulnerabilities there is the transfer of data from one server to another through a used USB memory stick, filming IT experts while typing passwords etc. During EFOR's observation mission in 2015 a few aspects were highlighted: operators kept sensitive passwords on pieces of paper in their pocket, the formal check of control keys (only the first and last digit of a code with dozens of characters), using communication services such as Gmail, working directly on root, without different access levels etc.

On the other hand, experts claim that the system is obsolete and cannot stand against new types of attacks. Moreover, votes can be modified if there is *malware* installed on the servers, even by officials. Also, such a virus installed on users' computers can change the votes, through stealing PINs or other personal data.

Estonian electoral authorities consider that this report is in mostly not well-founded. Even though they took into account the criticism included in the document, they claim the security of the system and the mechanisms of fighting against attacks are in place. According to them, the authors' tests were not even realistic, as they did not have access to the full source code.

There is criticism brought to the system also from within. A student committed fraud against his own vote and created the impression that the vote did not go towards the central system, after which he made the discovery public and brought the problem in front of the Supreme Court. The Court considered through Decision no. 3-4-1-4-11 that it is not fraud as it is about one's own vote; it is an incident similar to invalidation of a paper ballot. The Electoral Commission claims that they are permanently checking for these potential frauds and any deviation is seized and reported.

The OSCE/ODIHR reports have also included over the years multiple recommendations for system consolidation. Among these there is the usage of own qualified personnel by the Commission for electronic vote, clear rules for vote cancellation, possible attacks and crisis situations, and also for the destruction of votes, raising the process' transparency

7. Security Analysis of the Estonian Internet Voting System, *estoniaevoting.org*

LESSONS LEARNED OR WHAT ARE THE STEPS FOR INTRODUCING ELECTRONIC VOTING

Estonia must not be taken as given as an example of good practice; the model must be intensively discussed with pros and cons. There is a somewhat naivety in considering the Estonian system safe and replicable in other countries. There are multiple countries which looked at Estonians as an example, but adapted their own national specific procedures: Norway, Latvia, etc. Also in Romania, Estonia is seen as he Holy Grail of elections. Even so, Romania's conditions are very different: poor trust in parties and public authorities, raised size and fluidity of the electoral body (vs approx. 1 million voters in Estonia), electoral fraud as an extended phenomenon and a much larger number, as well as different profile of the diaspora. Let's not forget that in 2014 there was a case in which the ballot box was physically stolen from the polling station. Furthermore, we are not doing great at observing either, as the rules are pretty drastic, unfriendly to those interested; if we want electronic voting, surely these things cannot stay like this.

Even though political parties did not present very clear argument for electronic voting through internet vs voting by post, it seems that the latter instrument wins. The National Liberal Party already presented a project proposal. On the other hand, there were projects of laws on electronic voting and by post rejected by the Parliament, without much debate. The M10 Association launched an electronic vote project on 1st March (mzece.ro).

The arguments and public debates were accessories which politicians found dispensable for choosing the most appropriate distance voting system for diaspora. Real technical expertise lacked at party-level. A minimal comparative study and in general the discussions around electronic voting, naive and uninformed, were seen by parties more as a symbolic reverence towards the diaspora, which overturned the election result of November 2014. In reality, such a project cannot pass without consulting beneficiaries and electoral experts. We must learn from the lessons of those who succeeded or failed, including from our own pilot experiences.

Nevertheless, if we were to put internet voting in the public agenda, we must follow a few steps in order to assure ourselves that the result is the most appropriate one for the authorities and especially for the electors.

1. VISION, OBJECTIVES, POLITICAL CONSENSUS

First of all, we must establish what we really want to get from electronic voting. We consider that distance voting must fix the problem of the citizens that vote abroad, who do not have accessible means of voting. Without it being unconstitutional, electronic voting should not be included (at least for starters) for home electors, who benefit from different voting conditions.

Without political consensus, electronic voting can prove to a failure. The Latvian and Lithuanian cases are examples in this sense. Moreover, patience is a key element: in Estonia it took more than four years for the law to be passed by the Parliament and there were better preconditions than in Romania.

2. TESTING PERIOD, PUBLIC CONSULTATION

Electronic voting should not be implemented without having a clear plan: feasibility study, piloting, auditing necessary preconditions, ensuring the existence of necessary infrastructure. Public consultations must be a part of this process. Without consultations with beneficiaries and experts, legislation and system legitimacy is not ensured.

In Lithuania – a country without electronic voting – IT experts, with help from public administration developed a portal through which they tested electronic voting, www.ivote.it. This was developed before the parliamentary elections of 2012 in order to test the interest level for electronic voting. A number of 3566 people voted, and over 30,000 downloaded the application without voting[8].

8. *http://udris.lt/ivote/*

3. TAKING CARE OF THE LEGISLATION AND CONSTITUTIONALY OF ELECTRONIC VOTING

Following the Estonian example, before having a legislative formula, there must be a project proposal. The legislation must include very clear procedures for each step of the process, including voting procedures, system design, counting, vote destruction, crisis situations, invalid votes etc.

A preliminary discussion over the constitutionality of such a law is absolutely necessary. After the 2006 elections, the Netherlands quit using NEDAP voting machines after vulnerabilities were found in voting procedures and counting of votes. In 2010 they went back to classic voting, on paper ballots. The Federal Court of Germany took out of use in 2009 the voting machines, considering that it is unconstitutional, as long as the vote cannot be observed by any citizen, without technical knowledge. On the other hand, the Court considered that voting by post is constitutional, as facilitating the presence of electors to the vote is more important than the problems regarding security and vote secrecy. On the other hand, France completely eliminated postal voting in 1975 due to the potential for fraud.

Romania's Constitutional Court argued in Decision 61/2010 the fact that:

[...] a higher attention must be given to the possibility of Romanian citizens with voting rights who reside abroad, and not only to them, of exercising their right to vote, within the framework of a special procedure, including electronic voting, which should be conducted in correlation with the official hours in Romania when the voting process takes place.

4. ASSURING THE BASIC PRINCIPLES OF VOTING

In order to implement the system, **vote secrecy** must first of all be respected. The Romanian Constitution requires the vote to be secret. There have been intense discussions if home voting involves secrecy, as long as anyone can follow you when you vote or there are people who can constrain you to vote in a particular way. Estonians found a simple answer: every citizen is responsible for his/her own vote, and the one who breaks the principles can be sanctioned. The state cannot exhaustively ensure the secrecy, thus electoral bribe and influencing electors remain real problems. The electoral bribe and pressuring problems cannot be completely eliminated, but repeatedly expressing the vote is a solution. A citizen can vote electronically multiple times and just once in the voting station. The latest vote remains valid.

Individual and universal verifiability of the vote is essential. The voter must be able to check the fact that his/her vote was registered, then that it was registered according to his/her option, and finally counted as such. We presented two types of vote checking systems who offer this possibility to the voter.

Election observation is essential in order to ensure the citizens the possibility to check the procedures. Even though it is possible that a small number of citizens would be interested in the process, they must be able to observe every steps of the procedures, starting from pre-electoral system checks, to verifying and solving appeals. The Parliament has the opportunity to change current procedures (which are very dense and partially different from law to law) and to allow centralized accreditation by the Permanent Electoral Authority, valid throughout the country, the establishment of a special electronic register with observers and extending the categories of people who can register to citizens and political parties[9]. Eliminating the barriers against observers in Romania was mentioned in many OSCE/ODIHR reports.

5. CREATING INFRASTRUCTURE

Although in Romania it is highly unlikely to be able to introduce the Norwegian or Estonian model, documents with chips can be issued. For example, special cards with chips can be printed, secured by two codes – one for authentication and the other for confirmation. Some experts consider that for a country like Romania, this model is more practical, as it would eliminate the risk of fraud.

The state must ensure proper information and even qualification classes for citizens who want to use this system. Estonia invested European funds to teach its citizens how to use electronic instruments. We are not naive to think that Romania could reach the level of highly computerized countries,

9. See here EFOR's recommendations on this subject *http://expertforum.ro/recomandari-locale/*

especially since the level of internet access is lower than in most states who practice electronic voting, but efforts can focus towards target groups that are interested towards electronic voting.

6. TRANSPARENCY, SECURITY, PUBLIC TRUST AND SYSTEM EVALUATION

Transparency is the key to public trust in the authorities who organize electronic voting. According to current polls, political parties, the Parliament, but also the electoral administration suffer from chronic lack of trust. If political parties are assimilated to corruption and poor governance, the electoral administration does not have a profile that is visible enough among citizens.

In order to assure the transparency the Permanent Electoral Authority and the special commission for electronic voting must allow access to the public throughout the entire process. The software should be publicly distributed under an open format, and the voting, counting and electoral process finalization procedures must be very clearly specified and accessible by the public.

Developing the system should be done by consulting the civil society, the academic sector and through public debate. Selecting companies who would work on elaborating it, but also those who would offer the hardware infrastructure must be transparent, respecting the procedures. This step is very important as selecting a company who could influence the voting process could have a major impact on the elections.

The system management must be done by public institutions. In France, the system was developed and managed by Scytl, an international company known for electoral consultancy; still, the private management brought public dissatisfaction. Moreover, the source code was not made public and transparency procedures were not followed[10].

Human resources, as the Estonian experience shows, must be permanently prepared and high integrity standards must be introduced, in order to avoid any sort of incident. System evaluation must be able to be done by third parties. Auditing, evaluation and certification must be delegated to independent state organisms and must be published without exception. The audit must be done on the substance of the process and not just on documents or procedures. Election observation is one of the fundamental criteria established by the European Council for certifying electronic voting systems[11].

Security remains the taboo subject of this discussion. There are already sceptics among politicians and civil society, and the pros and cons can be equally valid for both sides. Nevertheless, there are a few preconditions of the electronic voting system which must be met in order to be able to talk about a minimal security. The encrypting model must be permanently checked and updated according to new technology. Tests are essential to discover system errors and vulnerabilities. Establishing clear rules and procedures, as detailed as possible, represents an opportunity of eliminating security systems.

10. E-voting in France*, https://vimeo.com/49293923*

11. Certification of e-voting systems Guidelines for developing processes that confirm compliance with prescribed requirements and standards, Strasbourg, 16 February 2011

SO, CAN ELECTRONIC VOTING BE IMPLEMENTED IN ROMANIA?

It's difficult to make predictions, especially about the future – Niels Bohr

The documented examples are very different and even though we have countries with a similar social, economic, technologic profile, we see different stands regarding electronic voting; and there are surely other models to discuss. There is no Holy Grail of electronic voting that can be applied, like a template for every country. In order to have electronic voting we must first of all see what are our needs and to establish from the beginning the fact that it is not so important to raise voting presence with new voters, but more to question how many electors would have participated at the November 20114 elections if there were electronic voting.

Even though it is a modern and accessible system, the problems regarding vote security must not be swept under the carpet, for they are very real and could have a major impact on the electoral process. The architecture of the project matters from the very beginning: encryption procedures, hardware and software, assuring vote secrecy or a good project management, with professional and upright staff. In the current situation, the beneficiary's interest must be placed ahead of the costs and thus we should not make savings who could jeopardize the project.

We must be realistic and see that neither the postal vote does not assure total secrecy, it cannot be easily observed and is not necessarily cheaper. If we follow the logic that paper is safer than a black box which we don't know how it works, then voting by mail is apparently safer. But the Romanian experience demonstrated that neither the paper ballot is safe from fraud. Imposing deterrent sanctions for electoral fraud must come along with introducing new types of distance voting.

One of the most convenient actions is testing electronic voting on elections with low stakes (or a referendum) in order to have a first experience to relate to. Discovering the most appropriate formula for Romania could take many years and we must not rush in adopting a fragile and corrupted system.

Voting must necessarily be in advance and not during election day. First of all, this would assure the possibility of remaking the elections in the case of an emergency situation. Moreover, it would offer more time to the public target we mentioned earlier, Romanian citizens abroad, to decide, but also to change their vote if desired. Being electronic voting and having registers with registrations, multiple voting is eliminated.

Shortly, electronic voting in advance could be implemented if all the previously mentioned phases – without them being exhaustive –, if all the necessary precautions are taken and if we start from some very clearly established objectives. And it could have a result only if it is taken through public debate, to whom all interested can participate. Electoral laws cannot be made in a dark office in the Parliament without a *reality check*.

NOTE

Expert Forum
12 Matei Millo Street, apt. 21, District 1
Buccharest, Romania
office@expertforum.ro
www.expertforum.ro