Ülle Madise

Professor of Constitutional Law
University of Tartu

Priit Vinkel

Assistant, University of Tartu
Advisor, Elections Department of the Chancellery of Riigikogu

Constitutionality of Remote Internet Voting:

The Estonian Perspective

1. Introduction

Estonia has used remote Internet-based voting in five elections: twice each in municipal and Riigikogu (parliamentary) elections and once in European Parliament elections. The number of 'I-voters' has grown sharply from less than 10,000 in 2005's municipal elections to over 140,000 in the 2011 parliamentary elections. The latter account for 24.3% of all votes cast and 56.4% of the advance votes. Initially, no individual complaints claiming unconstitutionality of I-voting were filed in court. In 2011, the situation has changed: critical public debate has re-emerged, followed by several complaints.

Only Estonia, Switzerland, Norway and a few other countries allow legally binding remote I-voting, though some countries are on their way toward its countrywide use. The list of countries that have abandoned the use of e-voting in various forms is much longer, including the US, Germany, Finland, and the Netherlands.[*1] France, for example, tries to keep alive the tradition of voting only at the polling station, as this ritualises citizenship[*2], but has allowed proxy voting and recently remote I-voting from abroad. The reasons for allowing or giving up on I-voting are different, but constitutional questions of whether fair and free voting can be secured in the case of remote I-voting have always been raised.

We are facing the pressure of the information society[*3]: people require e-services, yet, on the other hand, cyber-threats are more serious than ever before.[*4] Social changes have already forced countries to allow remote postal or proxy voting.[*5] We have to admit that holding on to old traditions (one single elec-

---

1 See the database for the Competence Center for Electronic Voting and Participation, at http://db.e-voting.cc/. German constitutional court decision to declare the use of voting machines unconstitutional: BVerfG, 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1-163). Available at http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html (9.10.2011). The core of the decision in German:

> *Der Grundsatz der Öffentlichkeit der Wahl aus Art. 38 in Verbindung mit Art. 20 Abs. 1 und Abs. 2 GG gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen.*
> *Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.*

2 L. Monnoyer-Smith. How I-voting technology challenges traditional concepts of citizenship: An analysis of French voting rituals. – R. Krimmer (ed.). Electronic Voting 2006: 2nd International Workshop Co-organised by the Council of Europe, ESF TED, IFIP WG 8.6, and E-Voting.CC. Bonn: Gesellschaft für Informatik 2006, pp. 63–64.

3 W. Drechsler. Dispatch from the Future. – The Washington Post, 5.11.2006.

4 J. Farwell, R. Rohozinski. Stuxnet and the Future of Cyber War. – Survival 2011 (53) 1, pp. 23–40.

5 See, e.g., the thorough overview of remote postal voting in N. Kersting. Briefwahl im Internationalen Vergleich. – Österreichische Zeitschrift für Politikwissenschaft 2004 (33) 3, pp. 325–328.

tion day, casting of paper ballots in a controlled environment as the only option, etc.) will not be possible in the future, but free and fair elections, anonymity of the vote, and the principle of uniformity must be guaranteed. The Council of Europe has adopted recommendation[*6] and guidelines[*7] for electronically enabled elections, and the OSCE/ODIHR is looking for ways to observe and evaluate various forms of e-voting, including I-voting. Estonia's I-voting experience is internationally followed with special attention; any failures would have very negative consequences not only for Estonian democracy but for all I-voting projects, worldwide.

The concept of the Estonian I-voting system is described and analysed here in the light of theoretical literature, judgements of the Supreme Court of Estonia, and the empirical data available. In addition to statistics, the results of sociological surveys are used.

2. Description of the concept of Estonian I-voting

Estonia's I-voting system is based on an electronic roll of voters, a compulsory e-ID, the public/private key infrastructure ('virtual double-envelope scheme'), and the right to change a vote given online ('virtual voting booth'). The elements of the system are meant to guarantee the compliance of the I-voting with constitutional principles of elections: only people entitled to vote can vote, access to voting shall be equal, one vote per voter shall be counted, free voting shall be granted, and both counting of the voting results and election results shall be fair and sound. Brief description of the elements of the Estonian I-voting system is given in this section; the constitutional analysis follows in Section 3.

2.1. Electronic Population Register

The Estonian Population Register is a uniform database of personal data of Estonian citizens and foreigners with Estonian residence permits. The Estonian voter roll is held on the basis of the Population Register, and voters do not have to enrol specially before elections. The Estonian electoral law[*8] states that electoral rolls are drawn up 30 days before election day but additions to the list can be made until the very end of elections. This gives the list the property of being constantly up to date in practice. During Internet voting, the voting roll is updated daily.[*9]

2.2. ID card and m-ID

The cornerstone of most e-services, public as well as private, is the e-ID.[*10] Since 2002, an ID card has been the new generation's mandatory primary identification document. The ID cards are issued by the government and contain certificates for remote authentication and digital signature. Every Estonian citizen or resident alien above age 15 must have an ID card.

Each ID card contains two discrete PKI-based digital certificates—one for authentication and one for digital signing. The certificates contain only the holder's name and personal code and have two associated private keys on the card, each protected by a unique user PIN. The certificates have no restrictions of use: they are by nature universal and meant to be used in any form of communication, whether between private persons or organisations or within the government. The e-ID card can be used also for encryption of documents so that only the person intended to view the document can decrypt it. This is an efficient means for

6 Recommendation on legal, operational, and technical standards for e-voting, Rec(2004)11; Recommendation on electronic democracy, Rec(2009)1. Available on the Council of Europe Web site.

7 Certification of E-voting Systems, GGIS(2010)3E; Guidelines on transparency of e-enabled elections, GGIS(2010)5E. Available on the Council of Europe Web site.

8 Up-to-date translations of election laws are available on the National Electoral Committee Web site: http://www.vvk.ee/?lang=en (9.10.2011).

9 For more information, visit the Web site of the Ministry of Internal Affairs, specifically http://www.siseministeerium.ee/35796/ (9.10.2011).

10 Detailed information about e-IDs, the areas of their use, etc. can be found at http://www.id.ee/?lang=en (9.10.2011).

secure transfer of documents over public networks. In addition, each ID card has all data printed on it also in electronic form, in a special publicly readable data file.

The number of ID cards issued grew in June 2010 to exceed 1.1 million. Over 2/3 of cardholders have used the e-ID card for remote personal identification and more than 1/3 for digital signature. Here it has to be noted that Internet voting has strongly promoted electronic use of ID cards. Another important promoting factor has been the agreement among banks to allow Internet banking only with an ID card or PIN calculator. The old password cards can be used only for very small transactions.

To use the ID card, one needs a smartcard reader and a computer with the relevant software installed (free for download from the Web page https://installer.id.ee/); an Internet connection; and a Windows, Mac, or Linux operating system.

A couple of years ago, a new e-ID solution was brought to the market: the m-ID, where a mobile telephone (via its SIM card) acts as an ID card and a card reader at the same time. In addition to having the functionality of an ordinary SIM, a mobile-ID SIM holds a person's mobile identity that enables providers of Internet services to identify the person and to issue digital signatures.[*11] Personal identification and digital signature functionality are secured by up-to-date security technology and corresponding personal identification numbers. Making the solution more convenient, with this, one does not need an ID card reader for the computer any longer; instead, one can perform electronic transactions just as one would with an ID card: it enables logging in to databases, Internet banks, etc. and signing various types of contracts digitally. The m-ID certificate is issued by the state and is thereby an equally e-enabled document to the ID card. The m-ID can be used as a means of authentication and digital signature in elections from 2011.

In practice, an e-ID is used for user authentication with several databases[*12]; the above-mentioned state portal serving as an e-service centre, e-tickets for public transportation, a customer loyalty programme identification tool in several private companies, and even insertion of comments for the online daily newspaper *Eesti Päevaleht*, which has prohibited anonymous comments in order to prevent libel cases. The use of e-ID is steadily widening, although the initial aim of combining e-ID with all possible other documents, such as driving licences, and replacing all possible password-based solutions has not been fulfilled yet.[*13]

2.3. System architecture

The Estonian IT security experts in their security analysis[*14] published in 2003 and revised in 2010 declared that in a **practical sense** the Estonian I-voting system was secure enough for implementation. In absolutely secure systems, unexpected events are not possible. One may dream about such systems, but they can never be realised in practice. This applies particularly to I-voting systems. Considering the security level of personal computers, it is impossible to design I-voting systems that are absolutely secure for every user. The most important security goal of voting is not to affect the final results and not to abuse the constitutional principles. Single incidents with users are still important, but they do not have an influence on the final result. Moreover, small-scale incidents are acceptable even in traditional voting systems.[*15]

The part of I-voting in the whole process of organising elections is relatively small. The system uses existing information systems—the Population Register for the polling list, election information system of the National Electoral Committee (hereinafter referred to as the NEC) for the collection and publication of information on candidates and voting results, and the infrastructure of Certification Centre Ltd. for checking ID card (or m-ID) certificates.

The main components of the Estonian I-voting systems are the voter application; the Vote Forwarding Server; and the back office, which is divided in two: the Vote Storage Server and the Vote Counting Application. These components support the following processes:

---

11 More about the m-ID project can be found at http://id.ee/?id=10995.

12 For example, the Estonian Research Portal, at https://www.etis.ee/index.aspx?lang=en, which compiles information on all Estonian researchers and their scientific projects, publications, and activities.

13 Comprehensive coverage of the ID card can be found in the work of T. Martens and E. Maaten. E-voting is here to stay. – Baltic IT&T Review 2006 (1).

14 Available from the NEC Web site at http://www.vvk.ee/public/dok/E-voting_concept_security_analysis_and_measures_2010.pdf.

15 T. Mägi. Practical Security Analysis of I-voting Systems. Master's Thesis 2007. Available at http://triinu.net/e-voting/master%20thesis%20e-voting%20security.pdf.

- The voter application is a Web-based application or an application on voters' personal computers.
- The Vote Forwarding Server is responsible for authentication, checking of enfranchisement, sending a list of candidates to voters, and receiving signed and encrypted ballots.
- The network server immediately transfers the received encrypted ballots on the Vote Storage Server and transfers the acknowledgements of receipt from the Vote Storage Server to the voters. The network server completes the work when the I-voting period finishes.
- The Vote Storage Server receives encrypted ballots from the network server and stores them until the end of the voting period. The Vote Storage Server is responsible for cancellation and management of votes.
- The Vote Counting Application is an off-line program that summarises all encrypted ballots. The encrypted ballots are transferred from the Vote Storage Server to the Vote Counting Application via data carriers. The Vote Counting Application does not receive voters' digital signatures, and it does not know voters' personal data.

Additionally, the I-voting system delivers independent log files, which consist of tracing data for the received encrypted ballots from the Vote Forwarding Server, all annulled encrypted ballots, all encrypted ballots sent to the Vote Counting Application, and all counted encrypted ballots. The cryptographic protocol used links all records in the log files. The NEC has the right to use the log files to resolve disputes. Hence, there is an independent audit trail to verify the e-voting process and help solve problems should they appear.[*16] The legality of all elections depends on the presence and proper functioning of these components.

2.4. Measures used to ensure voting secrecy

In order to understand how the I-voting system guarantees secret and equal voting, we should briefly describe the envelope voting method used in Estonia for advance paper voting. The latter gives the voter the possibility to vote outside the polling station for the voter's residence in any rural municipality or city. A voter presents a document for entry in the list of voters and then receives the ballot and two envelopes. The inner envelope has no information about the identity of the voter, and the ballot paper is put in it. The inner envelope is placed in an outer envelope, on which the voter's details are written, so that, after the end of the advance poll, the envelope can be delivered to the voter's polling station of residence. There it is verified whether the voter has the right to vote; then, the inner envelope is taken out and placed unopened into the ballot box. The two-envelope system guarantees that the voter's choice remains secret. The same system but electronically built is used in Internet voting.[*17]

Asymmetric cryptography is used to guarantee the secrecy of votes. A pair of keys is generated for the system in a special safety module so that its private component never leaves this environment. The public component of the pair of keys is integrated into the voter application and is used to encrypt the votes. The private component of the pair of keys is used in the vote-counting application to open the votes on the evening of election day. The NEC can open the votes—i.e., use the private component—only collegially. After the period for dealing with any complaints has elapsed, the private key is destroyed.

2.5. 'Virtual voting booth'

In order to guarantee the freedom of voting, I-voters have the right to replace the vote cast on the Internet by means of another I-vote or a paper ballot. However, this can be done only on advance polling days. In the case of several I-votes being cast, only the last one is counted; in the event of contradiction between an I-vote and paper ballot, the paper ballot is deemed definitive. If multiple physical ballots are cast, all votes are declared invalid.[*18] Thus the 'one voter—one vote' principle is guaranteed.

16 General description of the Estonian Internet voting system, 2010. Available at http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf (9.10.2011).

17 Details of the double-envelope scheme and description can be found in the General Overview document (Note 16).

18 Riigikogu Election Act (Riigikogu valimise seadus), §40 (6). – RT I 2002, 57, 355; RT I, 10.12.2010, 1 (in Estonian).

3. Analysis of the constitutionality of Internet voting

According to the Estonian Constitution*[19], members of the Riigikogu, as well as local government councils and the European Parliament shall be elected in free, general, equal, and direct elections, and voting shall be secret. There is no special regulation of I-voting in the Constitution. The legal framework for I-voting is laid down in electoral law. The provisions are almost the same in all legal acts regulating voting procedures. In the case of I-voting, almost all principles of democratic elections give rise to several questions in constitutional law and, more broadly, in social sciences.

3.1. A teleological interpretation of the principle of secrecy

The secrecy of voting has traditionally been viewed in Estonia as the right and obligation to cast one's vote alone in a voting booth. In the case of Internet voting, it is impossible to ensure the privacy aspect of the voting procedure. The voter's right to anonymity during the counting of the votes **can** be guaranteed, indeed to the extent to which this can be secured in the case of remote postal voting. Therefore, remote Internet voting requires rethinking of the privacy principle.

The principle of privacy is there to protect a person from any pressure or influence acting counter to his or her free expression of political preference. Such a teleological approach to the Constitution was the basis of the I-voting provisions from the very beginning of the whole project. In short, the provisions enabling Internet voting are based on the premise that the government has to trust the individual and avoid, whenever possible, interference with decision-making at the individual level.*[20] The individual has to be aware of the risks—e.g., technical risks—and he or she has to have the right to decide whether or not to exercise the Internet voting opportunity. The Supreme Court has agreed with this teleological approach to the principle of secrecy.*[21]

Buchstein, on the other hand, does not agree:

> Mandatory secrecy is a principle which goes beyond constitutional law, its fundaments are based on the idea of auto-paternalism and it is understood as a mechanism of self-binding of autonomous citizens in order to avoid situations of external pressure or corruption. In this concept, it is not the individual him- or herself, but a warranted outside agent or authority—normally the state—that is responsible for providing the necessary means to allow for the secret ballot.*[22]

Indeed, postal voting as another form of absentee ballot is widespread and is becoming accepted in Germany. There, the Federal Constitutional Court has twice declared remote postal voting to be constitutional, arguing that facilitation of voter turnout outweighs, in this case, the problems possible in relation to security and public scrutiny of electoral processes.*[23] In France, by contrast, postal voting was abolished in 1975 because of incidents of fraud.*[24]

---

19 Translations of Estonian legal acts can be found at http://www.just.ee/6906. Up-to-date official versions of all legal acts are available from the State Gazette, at http://www.riigiteataja.ee/ (in Estonian).

20 The ideological foundation and parliamentary debates are explored by W. Drechsler, Ü. Madise. E-voting in Estonia. – Trames 2002 (6) 3, pp. 234–244; W. Drechsler, Ü. Madise. Electronic Voting in Estonia. – N. Kersting, H. Baldersheim (eds.). Electronic Voting and Democracy: A Comparative Analysis. Basingstoke: Palgrave Macmillan 2004, pp. 97–108.

21 Available at http://www.nc.ee/?id=381 (9.10.2011).

22 H. Buchstein. Online Democracy. Is It Viable? Is It Desirable? Internet Voting and Normative Democratic Theory. – N. Kersting, H. Baldersheim (eds.). Electronic Voting and Democracy: A Comparative Analysis, Basingstoke: Palgrave Macmillan, pp. 39–58.

23 BVerfGE 21, 200 (15.02.1967); BVerfGE 59, 119 (24.11.1981). Available at http://www.wahlrecht.de/wahlpruefung/index.htm (9.10.2011).

24 L. Monnoyer-Smith (Note 2), p. 63.

3.2. Increase of turnout

One of the declared aims of launching online voting in Estonia was to increase voter turnout, which perhaps could be described more realistically as broadening access possibilities and stopping the decrease in participation. Scholars point out on the positive side of I-voting also that I-voting could and should better accommodate the needs of disabled voters.[*25]

The actual impact of Internet voting on the turnout does not lend itself to objective analysis. One can determine the variations of turnout in different election years (comparing equivalent types of elections) and attempt to clarify the causes underpinning variations with the aid of sociological studies. Perhaps the most important question is what proportion of the electorate would not have participated in the voting had the Internet voting opportunity not been provided. There does not exist a way of obtaining empirical evidence. We must, therefore, come to terms with unverifiable claims made by the voters themselves. The only exception is the case where Internet voting provides the only possibility for the elector to vote and he or she takes advantage of this possibility. For example, the local government council elections in Estonia do not provide the possibility of voting abroad by postal ballot or at a diplomatic representation. Nonetheless, it is possible to vote over the Internet when abroad.[*26]

Table 1. I-voting statistics for 2005–2011[*27]

	2005 LE	2007 PE	2009 EPE	2009 LE	2011 PE
Number of I-votes	9,681	31,064	59,579	106,786	145,230
Repeated I-votes	364	789	910	2,373	4,384
Number of I-voters	9,317	30,275	58,669	104,413	140,846
I-votes cancelled by paper ballot	30	32	55	100	82
I-votes counted	9,287	30,243	58,614	104,313	140,764
Total number of votes cast	502,504	555,463	399,181	662,813	580,264
I-votes out of all votes cast	1.9%	5.5%	14.7%	15.8%	24.3%
I-votes among total advance votes	7.2%	17.6%	45.4%	44%	56.4%
I-votes cast abroad (no. of countries)	n.a.	2% (51)	3% (66)	2.8% (82)	3.9% (105)

Source: National Electoral Committee

I-voting seems to have had, in 2005, a slight effect on the increase in the turnout of voters who sometimes vote and sometimes not.[*28] In 2007, approximately 10% of those I-voters questioned said that they certainly or probably would not have voted without having had the possibility to vote via the Internet. Moreover, Trechsel and Vassil show that the percentage of the I-voters questioned who certainly or probably would not have voted without having had the possibility to vote via the Internet has risen to 16.3%, which allows the conclusion that the overall turnout might have been as much as 2.6% lower in the absence of such a method of voting. That is already a significant marker when one looks at the impact of Internet voting on the overall turnout.[*29]

25 See, e.g., M. Loncke, J. Dumortier. Online voting: A legal perspective. – International Review of Law, Computers & Technology 2004 (18) 1, pp. 60–61.

26 Ü. Madise, E. Maaten. Internet Voting in Estonia. – D. R. Insua, S. French (eds.). Advances in Group Decisions and Negotiation Vol 5 e-Democracy: A Group Decision and Negotiation Perspective. Dordrecht, Heidelberg, New York, London: Springer 2010, pp. 314–316.

27 LE—Local Elections, PE—Parliament Elections, EPE—European Parliament Elections.

28 F. Breuer, A. Trechsel. E-voting in the 2005 local elections in Estonia: Report for the Council of Europe 2006, available at the Council of Europe Web site.

29 A. Trechsel, K. Vassil. Internet Voting in Estonia: A Comparative Analysis of Four Elections Since 2005. Council of Europe and European University Institute 2010. Available at http://www.vvk.ee/public/dok/Report_-_E-voting_in_Estonia_2005–2009.pdf (9.10.2011).

3.3. Uniformity

3.3.1. The digital divide and equal opportunities for representation

Trechsel *et al.* concluded in the report prepared for the Council of Europe following the experience of the Internet voting in 2005 and 2007 that education and income, as well as type of settlement, are insignificant factors in the choice of Internet voting over other voting methods. One of the most important findings of that study was that it is not so much the divide etc. between the Internet access 'have's and 'have-not's as, clearly, computing skills, frequency of Internet use, and trust in the I-voting procedure that direct voters' decisions to use or not use I-voting. Age has remained a significant factor for some years.[*30] Moreover, some interesting conclusions have been drawn in the latest report by Trechsel and Vassil, in 2010, where they state that the ICT variables (computing knowledge and frequency of Internet usage) have disappeared since the 2009 elections as predictors of Internet voting usage.[*31]

In the discussion of equal access to the place of voting, some authors[*32] ignore the fact that in Estonia there are quite many different voting methods; for example, if a voter is unable to vote at a polling place as a result of his or her state of health or for another good reason, he or she may apply to vote by paper ballot at home on the day of election day (Riigikogu Election Act, §46 (1)).

The Estonian Supreme Court has stated:

> The principle of equal treatment in the context of electing representative bodies does not mean that absolutely equal possibilities for performing the voting act in equal manner should be guaranteed to all persons with the right to vote. In fact, those who use the different voting methods provided by law (advance polls, voting outside the polling division of residence, voting in custodial institutions, home voting, voting in a foreign state, etc) are in different situations. For example, the voters who have to use the possibility of advance polls, are in a situation different from that of the voters who can exercise their right to vote on the election day. The guarantee of absolute actual equality of persons upon exercising the right to vote is infeasible in principle and not required by the Constitution.[*33]

In the future, the number of people without Internet access will probably decrease, but the digital divide is going to be even deeper than before. People without Internet access will have significantly less information, no access to voting-advice applications, etc. In this case, it is not the access to I-voting (as long as other methods of voting remain) but access to the candidates' and parties' information that might be the constitutional problem.

3.3.2. Impact on the voting results

The most intriguing question for political parties is probably that of the impact of the use of I-voting on results. Impact on the voting results can result from the fact that votes cast by those voters who would not participate if I-voting did not exist may not be distributed proportionally over the political spectrum. However, studies have shown that the left–right auto-positioning of the voter does not play any important role in the choice of a voting channel. The same applies to the 2009[*34] and 2011 elections.

30 A. Trechsel. Internet voting in the March 2007 Parliamentary Elections in Estonia: Report for the Council of Europe, 2007. Available at http://www.vvk.ee/public/dok/CoE_and_NEC_Report_E-Voting_2007.pdf.

31 A. Trechsel, K. Vassil (Note 29).

32 See, e.g., S. Meagher. When Personal Computers Are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights. – American University International Law Review 2008/23, pp. 374–376.

33 CRCSCd, 1.9.2005, 3-4-1-13-05, paragraph 24. Available at http://www.nc.ee/?id=381 (9.10.2011).

34 A. Trechsel, K. Vassil (Note 29).

Table 2. Relationship of I-votes to all votes cast for a political party

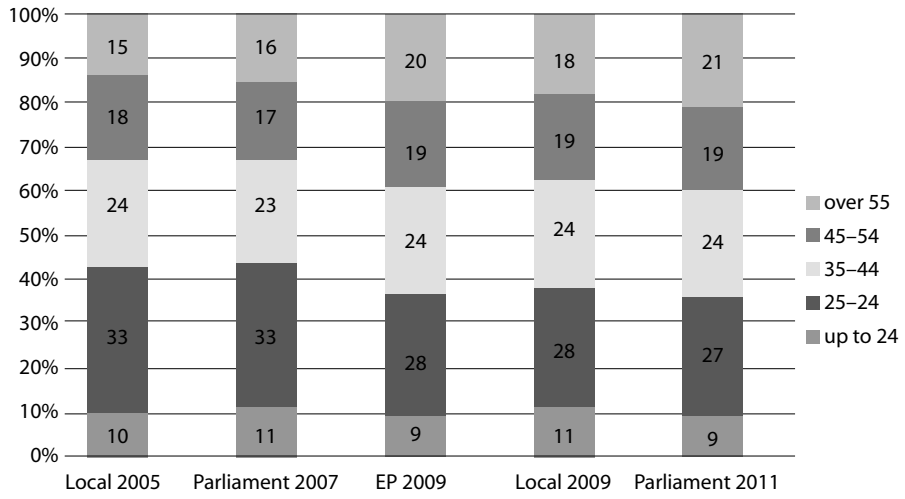
	2005 LE		2007 PE		2009 EPE		2009 LE		2011 PE	
	a)	b)	a)	b)	a)	b)	a)	b)	a)	b)
RP	32.7	3.6	34.5	6.8	20.1	19.3	25.1	23.7	37.0	**31.7**
PRU	10.4	2.3	26.7	**8.2**	17.3	**20.9**	22.5	25.5	25.4	30.3
PP	17.5	**3.8**	-	-	-	-	-	-	-	-
SD	9.9	2.9	13.3	6.9	10.4	17.6	10.7	22.6	18.0	25.8
GP	-	-	10.7	**8.2**	3.3	17.9	2.0	**27.4**	4.3	28.0
CP	8.7	0.6	9.1	1.9	10.9	6.2	14.7	7.4	9.9	10.4

Data: National Electoral Committee

a) = Percentage of I-votes
b) = Proportion of I-votes to total votes, in per cent
RP = Reform Party
PRU = Pro Patria and Res Publica Union (in 2005 only Res Publica)
PP = Pro Patria Union (merged with Res Publica to form PRU since 2007)
SD = Social Democratic Party
GP = Green Party
CP = Centre Party

In comparison of the overall distribution of votes in Internet voting or e-votes with that for total votes, not only the growing proportion of e-votes could be observed. According to Table 2, the party that is most popular in electronic voting is not always the one that profits the most from e-voting. The PRU (PP) and the GP (instead of the winner, RP) have been the greatest beneficiaries of Internet voting. The small numbers of e-votes on the account of the otherwise popular CP can be explained by that party's strong opposition to Internet voting from the very beginning[*35] but probably also by specifics of the electorate.

The hypothesis that I-voting rewards advantages to urban voters found no proof. Gender is also not an important factor when one chooses I-voting from among the possible voting channels. Age, by contrast, is quite an important factor in choosing Internet voting.[*36] Yet still, as can be seen in Figure 1, no age group is clearly dominant. The 55+ age group, with up to 20% of all Internet voters, is worthy of note here. So, while being younger correlates with use of the Internet as a means of voting, age does not give all the answers.



(Source: National Electoral Committee)

Figure 1. Age of I-voters in 2005 to 2011

35 Ü. Madise, E. Maaten, P. Vinkel. Internet Voting at the Elections of Local Government Councils on [sic] October 2005, Report on Internet voting to the NEC, 2006. Available at http://www.vvk.ee/public/dok/report2006.pdf (9.10.2011).

36 A. Trechsel, K. Vassil (Note 29).

It is, nevertheless, very interesting to compare the age groups taking part in Internet voting with the general electorate. For lack of a more comprehensive reference, we examine survey data from an exit poll conducted at the 2007 parliamentary elections by the Tartu University Department of Political Science.*[37] According to the poll the age groups break down as follows: ages up to 24 accounting for 12.3%, 25–34 for 16.3%, 35–44 for 19.5%, 45–55 for 16.5%, and over-55s for 35.4%. When comparing these figures to the Internet voting results for 2007, we see a strong over-representation in the under-35 group and under-representation in the over-55 age group. This appears to be consistent with the importance of age in the decision to choose Internet voting as a voting method.

3.3.3. The right to change one's I-vote

The President refused to promulgate amendments, which allowed I-voting and gave to the I-voter the right to replace I-vote once given with another I-vote or paper-ballot, to the Local Government Council election act*[38], arguing that I-voters are in a better position when compared to other voters, who do not have any right to change their vote once cast.*[39] The initial version of the I-voting law included the possibility of changing the I-vote with a paper ballot not only during advance voting but also on election day. To solve some of the problems indicated by the President, the Riigikogu restricted the time of I-voting to advance voting days. The chance to change their election preferences on Sunday after receiving additional information about candidates in the second half of the week had really placed I-voters in a better position. After this change, all voters who take advantage of advance poll possibilities were formally acting in the same conditions. The President did not see these changes as sufficient and initiated constitutional review.

The Supreme Court Chamber of Constitutional Review pointed out that, despite repeated electronic voting, there was no possibility of an I-voter affecting the voting results to a greater degree than can those voters who use other voting methods. From the standpoint of the voting results, this vote was deemed in no way more influential than a vote cast by paper ballot.

The most important arguments of the Supreme Court were the following. The principle of freedom of the vote gives rise to the obligation of the state to protect voters from persons attempting to influence their choice.

The aim of increasing voter turnout is without any doubt legitimate. The measures the state takes for ensuring the opportunity to vote for as many voters as possible are justified and advisable. Another aim in allowing I-voting is the modernisation of voting practices that coincides with the aims of I-voting listed in the recommendation Rec(2004)11, on legal, operational, and technical standards for I-voting, of the Council of Europe.

In accordance with the Penal Code, preventing a person from freely exercising his or her right to elect or be elected in an election or to vote in a referendum, if such prevention involves violence, deceit, or threat or takes advantage of a service, economic, or other dependency relationship of that person with the offender, is punishable by a pecuniary punishment or up to one year of imprisonment. The possibility for the voter to change the vote cast by electronic means throughout the advance polling period constitutes an essential supplementary guarantee to the observance of the principle of free elections and secret voting upon voting by electronic means.

A voter who has been illegally influenced or watched in the course of electronic voting can restore his or her freedom of election and the secrecy of voting by voting again, either electronically or via a ballot paper, after having been freed from the illegal influence. In addition to the possibility of subsequently rectifying a vote given under such influence, the possibility of voting again serves an important preventive function.

---

37 R. Toomla. Results of 2007 Riigikogu elections exit polls. Conducted by the Department of Political Science of Tartu University. Unpublished, available to the authors.

38 Draft No. 607 SE in X Riigikogu proceedings. The draft, information regarding parliamentary procedures, and motions to change the draft are available on the Parliament Web site at http://www.riigikogu.ee/?page=eelnou2&op=ems&eid=607&assembly=10&u=20110420131938 (9.10.2011) (in Estonian). The I-voting provisions were first adopted as a law in 2002; see drafts 747 SE, 748 SE, 771 SE, and 906 SE in IX Riigikogu proceedings. Right before the very first use of I-voting in 2005 municipal elections, the Riigikogu decided to change some I-voting provisions and the President used his suspensive veto foreseen in §107 of the Constitution of Estonia.

39 Decision No. 873, 22.6.2005. Available at http://vp2001-2006.president.ee/et/ametitegevus/otsused.php?gid=64640 (in Estonian).

When the law guarantees a voter who is voting electronically the possibility of changing a vote cast by electronic means, the motivation to influence him or her illegally decreases.

There are no measures as effective as the possibility of changing a vote cast by electronic means for guaranteeing the freedom of election and secrecy of voting upon electronic voting by means of an uncontrolled medium. The infringement of the right to equality and of uniformity, which the possibility of I-voters to change their vote an unlimited number of times can be regarded as amounting to, is not sufficiently intensive to outweigh the aim of increasing participation in elections and introducing new technological solutions.*[40] Norwegian scholars arrived at similar principles independently before obtaining in-depth knowledge of the Estonian Internet voting system.*[41]

In fact, the number of changed and replaced votes has been low in all elections. The maximum number of replaced votes has been 100, and the percentage of repeated votes does not exceed 4% of total e-votes.*[42] So, any fears of misuse of these opportunities cannot be validated.

In short, the fact that the Internet voter is in a somewhat different position from the traditional voter does not in itself indicate an infringement of the constitutional values. The Supreme Court thus confirmed the constitutionality of one of the main premises of the remote Internet voting project.

3.3.4. Computing skills and security of the voter's computer

It has been noted that good computing skills have been an important factor in choosing Internet voting as a mode of voting in the 2005 and 2007 elections. Since 2009, the ICT variable has lost its meaning in defining the reasons behind the choice of using e-enabled voting. However, since the absolute number of Internet voters has steadily risen, the question of technical uniformity and usability emerges. I-voting has been offered in a variety of environments and on several platforms claiming to cover the maximum number of possible voters. In addition, comprehensive informational materials and a 24-hour help line are available.*[43] However, a peculiar issue arose in the 2011 elections. There were a few voters who used a very rare combination of screen resolution, Windows 7, and font sizes on their computer. When these people used the Internet voting application, some of the interface and control buttons were left behind the Windows taskbar. This would not have been a greater problem unless some of the candidates' names too were covered by the taskbar. One of the candidates brought a complaint to the Supreme Court that stated:

> The chamber adds that in organising Internet voting the state has to guarantee the accordance of the application with most common hardware, operating systems, resolutions, and fonts. In some cases, compliance cannot be guaranteed. In the event of such problems, the voter has the option of contacting the technical support staff. If the issues cannot be resolved, the voter can use the traditional means of voting.*[44]

Therefore, ensuring the compatibility of the computer with the Internet voting application is clearly left to the user.

The security analysis of the Internet voting concept*[45] states clearly that one of the fundamental security problems with electronically enabled voting is the necessity of trusting the voters' computer. The central system can be, and is, protected by the state. The spread of malware on private computers, on the other hand, cannot easily be limited—either by the state or through private efforts. The analysis even says that the modern personal computer is a 'black box' that nobody is able to control. Therefore, the security of the computer on which the voting application is run remains an issue in actuality. The user—the voter—can, of course, take actions to protect the computer, but, nevertheless, this cannot resolve all possible consequences. Accordingly, the security of the voting application is a topic that is being given extra attention.

---

40 CCRSCd, 1.9.2005, 3-4-1-13-05 (Note 33).

41 G. Skagestein, A. V. Haug, E. Nodtvedt, J. Rossebo. How to create trust in electronic voting over an untrusted platform. – R. Krimmer (ed.) (Note 2), p. 108.

42 See Table 1 for further data.

43 Available at http://www.valimised.ee/internet_eng.html (9.10.2011).

44 In 3-4-1-6-11. Available at http://www.riigikohus.ee/?id=11&tekst=RK/3-4-1-6-11 (in Estonian).

45 See Note 14.

However, the issue of secrecy became prominent during the 2011 elections when a computer enthusiast hacked his own vote in the voting application on his own computer. He was able to modify the vote and create an illusion of the vote not having been sent to the central system. He was also keen to go public with his discovery (to national media) and later bring the issue up to the Supreme Court. It is important to state that all of the problems and situations discovered were monitored in the central system and that the threats revealed had been discussed already in the 2003 security analysis.

Subsequently, the Supreme Court, in its judgement No. 3-4-1-4-11[*46], stated that knowingly manipulating one's own vote cannot be seen as grounds for indictment of the overall security of the Internet voting system. In an analogy with traditional voting, a voter could easily go to the polling booth and make the polling paper invalid (by scrapping or doodling on the paper, etc.). That is a conscious decision and is completely legitimate.

However, the debate about secrecy is never resolved. Another issue that was raised by the computer enthusiast described earlier is the traceability of a vote. The reasoning behind this is that the online environment cannot be trusted and additional external proof of compliance has to be generated. A very interesting Internet voting pilot project is to be introduced in late 2011 in Norway.[*47] In this project, external means of confirming one's choices are used. Namely, voters receive a special printed polling card (by post) with all candidates who are running for election represented by code names. After voting, the voter can request the code name matching the vote cast, via independent channels. This should, in theory, guarantee that the vote can be traced and that it has been accepted.

However, some additional concerns arise with this. Firstly, new channels of communication have to be built and secured between the state and the voter. Secondly, issues with the principle of anonymity come up where the voter has to understand that under some circumstances the state knows how he or she has voted. Thirdly, how does this traceability affect the possibility of buying or selling one's vote over the Internet?

4. Certification and auditing

Certification is, in broader term, a process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it at least includes provisions for ascertaining that the system is functioning as intended. This can be done through measures ranging from testing and auditing to formal certification. The end result is a report and/or a certificate. An audit is an independent pre- or post-election evaluation of a person, organisation, system, process, entity, project, or product, which includes quantitative and qualitative analysis.[*48]

Currently, there is no domestic or international public body that would be ready to certify and audit all the elements of an entire I-voting system before, during, and after election procedures. In Estonia, hired specialists performed comprehensive tests in order to check the functionality and accuracy of the system both as experienced by testers and in public (in demo voting). A third party audits the source code and the procedures that have been carried out.

The Estonian I-voting system was developed to follow the principle that all components of the system must be transparent for audit purposes. Procedures should be fully documented, with those that are critical being logged, audited, observed, and videotaped as they are conducted. A common requirement is that the source code of the voting application be available for auditing. In Estonia, though the code is not universally available, it could be audited if so agreed by the NEC.

As a rule, the process audit is ordered from external internationally certified IT auditors. The audit reviews and monitors sensitive aspects of the process, such as updating of the list of voters, preparation of hardware and its installation, loading of election data, maintenance and updating of election data, and the process of counting the votes etc. At the counting event on election day, auditors publicly declare their opinion about the soundness of the procedures of the electoral administration to that point. The report of the auditors, released after all procedures are complete (including the destruction of all voting equipment—

46 Available at http://www.riigikohus.ee/?id=11&tekst=RK/3-4-1-4-11 (9.10.2011) (in Estonian).

47 For more information about the Norwegian Internet voting system, see http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658 (9.10.2011).

48 Council of Europe Rec(2004)11 and guidelines based on that recommendation (see Note 7).

I-votes along with it), states whether the I-voting procedures followed the rules described in the system's documentation and whether the integrity and confidentiality of the system was not endangered. To date, all reports have been positive.

The I-voting system produces a wealth of system log information that can be used to monitor the work of the system thoroughly. In its different stages, the I-voting system produces a variety of logs concerning received, cancelled, and counted votes, also invalid and valid votes. The audit application enables determining what happened to an I-vote cast by a specific person without revealing the voter's choice. These logs provide external auditors as well as observers with information that they can use to ensure that the system is working correctly.

According to the Estonian electoral laws, all activities related to elections are public. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting process, the counting, and tabulation of results. Internet voting is no different. All significant documents describing the I-voting system are public. In order to enhance the observers' knowledge of the system, the political parties are invited to take part in a training course before each election, in which I-voting is used. Besides political parties, auditors and other persons interested in the I-voting system take part in the training. In addition, observers are invited to follow the testing of the whole process and take part in other preparatory procedures. However, few political parties have so far exercised their opportunity to observe the I-voting procedures.[*49] It is important that observers be deployed for an amount of time that suffices to allow meaningful observation. If some important stages influencing the correctness of final results have not been observed, conclusions cannot be made as to the integrity of the system.

The OSCE did audit the 2007 elections, and in its report it states that the "election administration implemented the [I-voting] system in a fully transparent manner, and appeared to take measures to safeguard the conduct of Internet voting to the extent possible".[*50] Professional, independent, reliable, and comprehensive IT audit and certification procedures should compensate for the lack of simple public scrutiny.

5. Conclusions

In Estonia, as well as in many other countries that have prepared systems for, and allowed, postal voting, advance voting, and other supplementary voting methods, voting at a polling station has virtually lost its significance as a ritual of transforming people into a nation-state and a carrier of sovereign nationhood.

In discussion surrounding the introduction of I-voting, the classical arguments concerning the conformity of I-voting with the principles of fair elections (including the reliability of the electronic voting systems) have gained renewed force. For example, one of the typical arguments against I-voting is that people who have no commitment to go to the polling station to execute their citizen's duty should not participate in governing at all, which contradicts the axiom that the higher the turnout the better.

A possible lack of legitimacy of the election results could result from either of the following situations:

- The privacy of individual I-voting procedure cannot be supervised by authorities or observed in a traditional way. Therefore, massive buying and selling of votes, as well as exercise of other influence or pressure on the voter, is possible.
- The people themselves cannot verify the I-voting results, and people need to have absolute faith in the accuracy, honesty, and security of the whole electoral system (its people, procedures, software, and hardware) if it is to be legitimate. For people who didn't take part in developing the system, the computer operations can be verified only by knowing the input and comparing the expected with the actual output. In a secret ballot system, there is no known input, nor is there any expected output with which to compare the electoral results.[*51]

Therefore, the question of whether remote Internet voting with binding results in public political elections complies with the constitutional principles of fair voting cannot be answered simply with a 'yes' or

49 E. Maaten, T. Hall. Improving the Transparency of Remote I-voting: The Estonian Experience. – R. Krimmer, R. Grimm (eds.). Electronic Voting 2008, Gesellschaft für Informatik. Bonn 2008, pp. 31–43.

50 OSCE/ODIHR 2007. Election Assessment Mission Report, Republic of Estonia, Parliamentary Elections, 4 March 2007. Available at http://vvk.ee/public/dok/OSCE_report_EST_2007.pdf (9.10.2011).

51 Ü. Madise, T. Maaten (Note 26).

'no'. Actually, the question and answer should be divided into two parts. The first sub-question should be whether the legal norms in the abstract comply with the constitutional provisions and the second whether the technical solution used to conduct voting procedures in a certain election guarantees constitutionality.

The first sub-question can be answered on the basis of theoretical analysis, but the second should be examined before and after the relevant elections. The fact that it is possible not to fulfil the legal requirements set for an I-voting system is not enough *per se* for declaring I-voting as a concept unconstitutional. As a matter of fact, this underscores the importance of qualified certification and auditing of the system as well as the need for a new approach in electoral observation. The second sub-question can be answered with a 'yes' only if sufficient measures are in place to check whether the IT solutions work properly. This leads to a requirement that auditing, certification, and evaluation as required in the Council of Europe guidelines*[52] be foreseen by law or NEC regulation.

In the Estonian case, the first sub-question could be answered 'yes', as e-ID enables secure remote identification, e-ID has wide penetration, all advance voters are placed in the same conditions, and the 'virtual voting booth' (the right to replace an I-vote with another I-vote or a paper ballot) and 'virtual double-envelope system' ensure freedom of voting and uniformity of elections. Moreover, the system is justified by the aim to guarantee universal suffrage in an information society where e-services (including Internet voting) are demanded by a significant proportion of the electorate. Whilst formal equality can be provided, the questions of material equality and the issue of the digital divide remain. In addition, complying with the principle of secrecy poses new obstacles for many countries. According to the above teleological interpretation of the principle of secrecy, the voting act is to be seen not as an aim but as a measure to guarantee freedom of voting, and the anonymity aspect of the principle of secrecy can be guaranteed. The analysis of the compliance of the Estonian I-voting system with the United Nations International Covenant on Civil and Political Rights has given positive result as well*[53] but emphasises the importance of special procedures to facilitate auditing and observation of I-voting.*[54]

The answer to the second sub-question is more complicated. Internet voting in concrete election is constitutional if the provisions of the law are fulfilled in practice: only people entitled to vote can vote, e-votes cast over the Internet are recorded and counted properly, and only one vote per voter shall be counted. Independent IT auditing that covers all aspects of the system can prove its soundness. The proper performance of the IT system should be certified and audited before, during, and after voting. The personal computer and the Internet remain a weak point of the system. The scholars are probably right in saying that "[a]lthough perfect real-time knowledge of all cyber threats is an impossible goal, it *is* realistic to do mach better at providing a richer, better integrated picture of our cyber security to the technologists, attorneys, and political leaders who will have to collaborate to avert the next cyber attack".*[55] Both new threats and I-voting are part of the information society.

52 See Note 7.

53 S. Meagher (Note 32), pp. 349–380.

54 *Ibid*., pp. 384–386.

55 Th. C. Wingfield, E. Tikk. Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen. – International Cyber Security. Legal & Policy Proceedings. Tallinn: CCD COE Publications 2010, p. 21.