DOI:10.1515/curie-2015-0022

ANNALES
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA
VOL. XXII, 1 SECTIO K 2015

Adam Mickiewicz University in Poznań, Poland

MAGDALENA MUSIAŁ-KARG

Implementation of electronic voting and the matter of security[1]

ABSTRACT

Electronic voting (as well as computer-aided voting) is an interesting subject for many countries around the world. The idea to implement e-voting into elections and referenda is widely discussed not only by members of parliaments and governments throughout the world but also by regular voters, IT specialists, engineers or people who work in organisations/associations supporting application of ICT in government. This idea is strengthened by the fact, that e-voting is successfully applied in Estonia and Switzerland for several years. However, in some European states (e.g. in the Netherlands, Norway and Austria) the attempts to implement that form of participation in elections fell out to be unsuccessful.

This article aims at providing an answer to the question about the matters of security during implementation of electronic voting systems, which are more and more popular as an additional form of voting during elections or referenda. The theoretical context of the considerations is based on the concepts of electronic democracy (as a new paradigm of democratic power in contemporary states) and voting supported by ICT (understood as the essential tool for e-democracy). Apart from theoretical considerations on the e-voting itself, this text includes references to the most important motives that accompany e-voting implementation and then it delivers arguments on various aspects of security within the e-voting system.

Key words: electronic voting, security, ICT

[1] Paper prepared under the scientific project entitled: *E-voting jako alternatywna procedura głosowania w elekcjach państwowych. Doświadczenia wybranych państw a perspektywy wdrożenia e-głosowania w Polsce [E-voting as an alternative voting procedure in state elections. Experience of selected countries and the perspectives of e-voting implementation in Poland]*: UMO-2014/15/B/HS5/0135 (NCN, program OPUS).

In the era of new technologies, it is common to see tendencies to merge the political sphere with development of ICT tools. The increased use of ICT promises at least to evolve (or even sometimes to revolutionize) both the provision of public services and the vibrancy of democracy. We observe more and more frequent instances of initiatives to introduce electronic forms of voting at the national level in Europe and the whole world.

The security of electronic voting and counting technologies are the key factors when e-voting systems are to be implemented. In particular, the issues of e-voting's security in the context of the electoral process is probably one of the most important constraints, that raises concerns about the secrecy of ballots in general election. The electronic technologies employed in voting procedures are inherently less transparent than the use of traditional paper ballots, 'where all steps of the voting and counting process are observable' [Goldsmith, Ruthrauff 2013: 136] and they seem to be much easier to control than the methods based on ICT. If the e-voting systems are to be trusted by electorate, it is the key issue to make the security procedures and challenges understandable for the electoral stakeholders and to make the act of voting secure beyond any reasonable doubt.

This article aims at providing an answer to the question about the matters of security during implementation of electronic voting systems, which are more and more popular as additional form of voting during elections or referenda. In this paper, I focus on the security related issues that are usually required in the context of development and deployment of e-voting in legally binding general elections.

The theoretical context of the considerations is based on the concepts of electronic democracy (as a new paradigm of democratic power in contemporary states) and voting supported by ICT (understood as the essential tool for e-democracy). Apart from theoretical considerations on the e-voting itself, this text includes references to the most important motives that accompany e-voting implementation, and then it delivers arguments on various aspects of security within the e-voting system (also on requirements that e-voting systems must meet).

ELECTRONIC VOTING – SOME DEFINITIONAL REMARKS

Electronic voting seems to be one of the most interesting examples of the application of security-sensitive information technology in contemporary democracies. In recent years governments in many countries have embraced the idea of using modern technologies (ICT) to improve services, 'a trend known as e-government' [Moynihan 2004: 513]. So, 'it is no wonder that the introduction of new technology into this domain has raised a considerable amount of discussion' [Pieters 2006: 283]. This is proved by the fact that every year in more and more countries possibility of implementation of electronic voting systems in elections is discussed. Additionally, good experiences of Estonia, Switzerland, Brazil or other states push other countries

interested in e-voting systems to make endeavors to test and implement systems of voting supported by ICT. The idea to implement e-voting into elections and referenda is widely discussed not only by members of parliaments and governments throughout the world but also by regular voters, IT specialists, engineers or people who work in organisations/associations supporting application of ICT in government.

Starting considerations on e-voting systems there is a need to define the notion of electronic voting. One should notice that there are many definitions of e-voting and it is relatively difficult to choose the best description of this term. One of the very general definitions is the one saying that 'E-voting can be defined as the use of electronic means to cast, record, and/or count votes. E-voting devices may include, for example, those in polling stations, Internet voting, mixed systems, voting by mobile telephone, and so forth' [The Carter Center 2012: 1]. 'An electronic voting system is understood as a voting system in which the election data is recorded, stored and processed primarily as digital information' [Al-Ameen, Talab 2013: 397].

According to the *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, adopted on 30 September 2004, electronic voting can be divided into two main categories: remote e-voting and remote kiosk voting. Remote electronic voting is a voting which takes advantage of electronic media, while the act of voting itself may take place anywhere. This type of voting may consist in voting through the Internet, a text

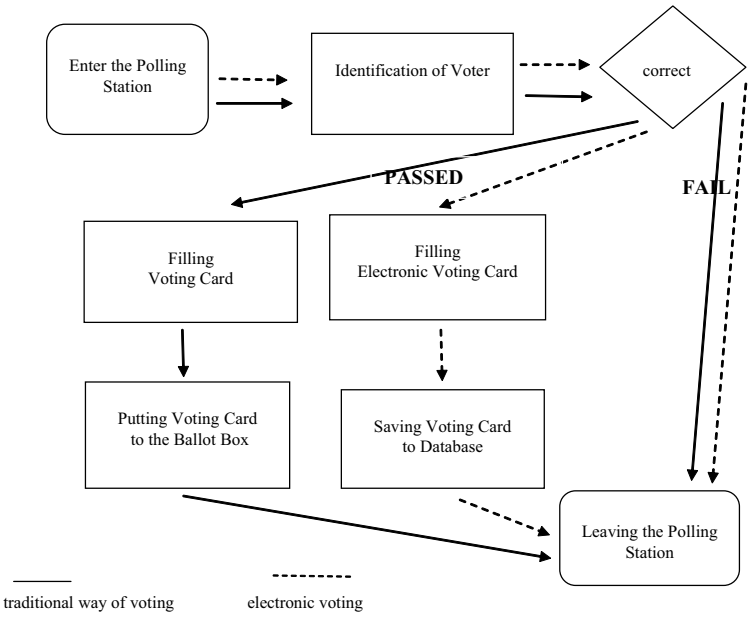

Figure 1. The classical voting process and e-voting at the polling place process

Source: own study based on: Al-Ameen, Talab 2013: 398.

message, and interactive digital television or phones with a touchscreen. Remote kiosk voting requires the voter to register his/her vote by visiting a polling station or other location specified by the election authorities [Mägi 2007: 12]. Votes are cast electronically – often through devices with a touchscreen. Votes are counted on separate devices called DRE machines (Direct Recording Electronic machines), and then transferred to the central register of cast votes.

One may state that there are two recognized types of electronic voting: the first one – e-voting at the polling station, and the second one – remote e-voting (using computers at remote locations). The process of voting in the classical voting act is very similar to e-voting at the polling station (see Figure 1).

Undoubtedly, e-voting is similar to traditional way of voting based on "paper-form" voting, where voters entering the polling station after successful identification can give their vote casting it to the ballot box. The process of voting in the so-called e-voting at the polling place looks similarly: after identification at the polling station voters are voting via pushing buttons on various electronic devices [Al-Ameen, Talab 2013: 398].

In the remote electronic voting voters give their votes via their own computers (from remote location) connected to the Internet (see Figure 2).

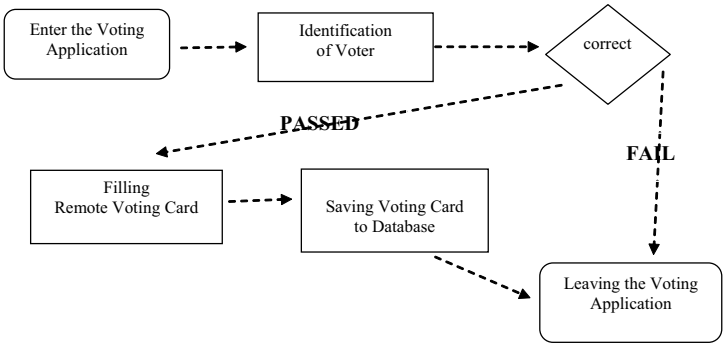

Figure 2. Remote e-voting process

Source: own study based on: Al-Ameen, Talab 2013: 398.

Specialized literature usually mentions two types of e-voting: electronic voting (*e-voting*) and Internet voting (*i-voting*). E-voting is a notion of broader meaning and includes the form of Internet voting. As it has already been mentioned, the electronic voting refers also to the application of e.g. digital television platforms, telecommunication and the Internet to the processes of voting technique [Nowina-Konopka: 2].

Internet voting can be divided into two categories: Internet voting at the polling place and remote Internet voting. As far as the first category is concerned, the voters cast their votes through the Internet in a specifically designed voting kiosk. On the other hand, remote Internet voting allows voting both from the 'voting kiosk'

(but located outside a polling station), or from a personal computer connected to the Internet. Data from each mentioned types of voting station is sent to the central database through the Internet.

It has to be mentioned that the Internet Society Poland *(ISOC)* has adopted the *statement on electronic voting during public elections* [2007] which emphasized that voting based on electronic methods is a notion of broad meaning, and telecommunication and information technologies are applied to electoral system in the following way:

- during the processes of collecting, developing and presenting results submitted by electoral committees, which votes are cast traditionally (on ballot papers);
- during the process of collecting and counting votes;
- during remote voting through the Internet.

Application of the ICT tools to the procedure of collecting and counting votes and to remote voting through the Internet is referred to as e-voting.

It is also worth mentioning here that all the forms of electronic voting (Internet voting as well) can be applied during any kind of general election (e.g. parliamentary, presidential or self-government elections). In such a case, the elections will be referred to as e-elections (electronic elections) or i-elections (Internet elections, i.e. elections through the Internet). In case of a referendum, the election would be referred to as e-referendum (electronic referendum), or i-referendum (Internet referendum) [Musiał-Karg 2014: 312; Musiał-Karg 2011: 104].

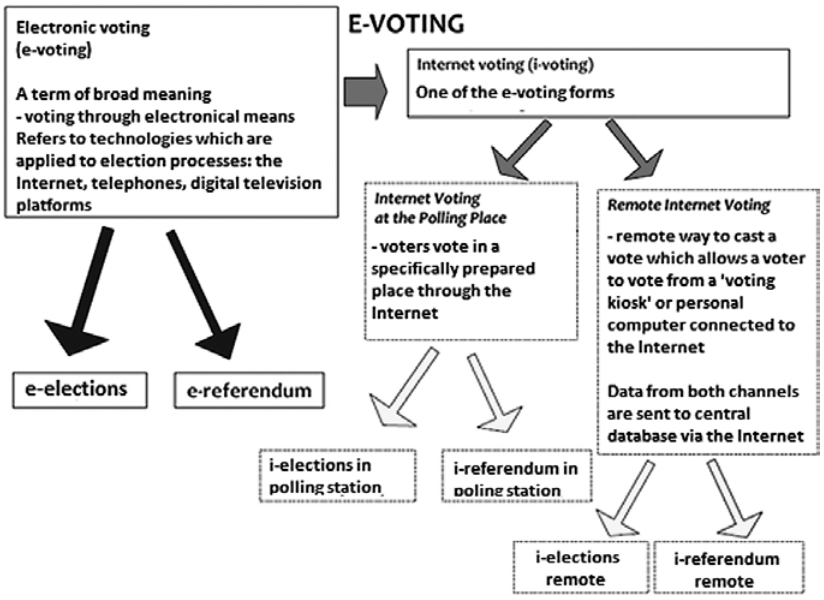

Figure 3. Forms of electronic voting

Source: own study.

Mentioning i-voting it is worth to remind that it may be analyzed from the perspective of three different methods: Internet voting through voting machines located within a polling station, through a voting kiosk located outside a polling station and through online remote voting (from a computer or a mobile phone).

The first method of Internet voting – voting in a polling station – guarantees high level of supervision, ensures a great degree of security, yet it is a less available method for the electorate in comparison with the other two types of Internet voting (i.e. a voter needs to visit particular polling place in order to cast the vote). Remote voting from a voting kiosk ensures moderate level of supervision (lesser than a polling station), high level of security, and the voting kiosk is more accessible for an average voter. It should be also mentioned that the method may generate more technical problems in comparison with the Internet voting method described in the first place.

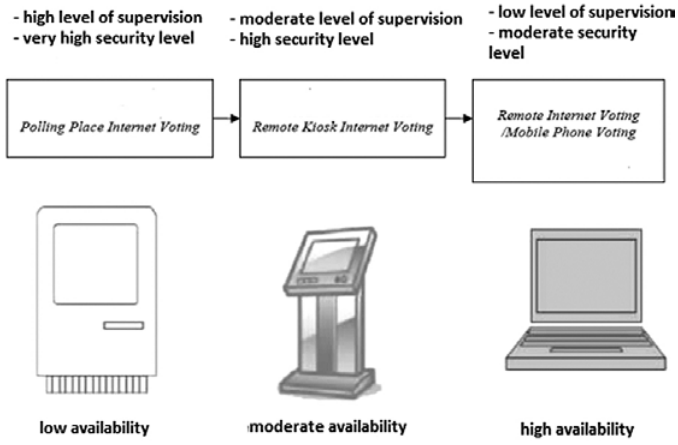

Figure 4. Methods of Internet voting

Source: *A Comparative Assessment of Electronic Voting*, http://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=description&lang=e#fg1 (access 11.10.2012).

Remote Internet voting through a computer or a mobile phone seems to be the method that is less susceptible to various types of technical problems (e.g. small number of users – voting through a computer or a mobile phone is usually conducted only by the owner of respective device). From the perspective of a voter, such voting may take place at any time during the day and from any place (thus, it is quite more available for the voter than the two latter voting systems). It is worth adding that remote Internet voting guarantees much lesser degree of supervision and it is impossible to ensure high level of security in this method – the security level should be rather described as low to moderate [*A Comparative Assessment*]. Distinguishing between representative democracy and direct democracy, we can identify two types of electronic voting: *electronic elections* (*e-elections*) and *electronic referendum* (*e-referendum*). As far as the technological requirements are concerned, the latter

manner of voting seems to be less complicated to introduce mainly because there are usually only two possible answers to choose from ('Yes' and 'No'). In case of elections, the ballot paper is usually more complex and extensive in terms of contents than the referendum paper.

The process of electronic voting can be divided into six key stages. The first stage – registration of voters – consists in defining the voters who are eligible to decide through electronic voting system and providing them with authentication data which are required to sign in the e-voting system.

The second stage aims at verifying whether the person, who signs in, actually has the right to access the system and the right to vote. In the third stage, an eligible voter casts a vote, and the e-voting system registers it.

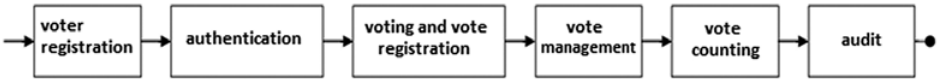

Figure 5. Stages of e-voting

Source: Mägi 2007: 16.

In the next stage, all votes are being appropriately sorted and prepared for counting. The counting phase involves deciphering them, and then counting and comparing them. The auditing stage aims at verifying whether the cast votes should be taken into consideration in the final results and the turnout. Importance of each stage of electronic voting is crucial from the perspective of the whole system credibility. Thus, each stage of e-voting should guarantee secure and correct operation of the whole e-voting system [Mägi 2007: 16].

ELECTRONIC VOTING: THREATS, SECURITY CONSTRAINTS. PROS AND CONS OF E-VOTING

Security is one of the most important problems regarding the electronic voting, because 'without proper protection and effective control procedures, malicious actors may instantiate a range of threat actions, with effects varying from a "denial of service" (e.g. stopping the election in a polling station by sabotaging some e-voting machines) up to alteration of the results (e.g. by successfully changing votes in some key precincts)' [Weldemariam, Villafiorita, Mattioli 2007: 38].

Security in e-voting is a problem because, the available technology does not guarantee a completely secure e-procedural environment. Thus, one may assert security is a kind of technological problem. The Communications-Electronics Security Group in the UK (CESG) when dealing with e-voting security, considers it 'to be related to a set of principles including voter authenticity, voter anonymity, data confidentiality, data integrity, system accountability (operations are logged and audit-

ed), system integrity (not to be able to reconfigure the system during its operation), system disclosability (allowing external scrutiny), system availability (encountering accidental or malicious denial of service attacks), system reliability (developing non-problematic systems), personnel integrity along with operator authentication and control' [Xenakis, Macintosh 2004: 2].

When discussing the issue of security of electronic voting one should remember that the secure environment of e-voting is dependent on many factors influencing the electoral process. Secure environment of e-voting depends on the voting technology used to provide alternative voting channels (kiosk voting, sms voting, digital television interface voting, Internet voting, etc.). The second important factor is the commercial vendor supplied security checks. Security of the e-voting process depends also on the location from which voting takes place. 'Remote or unsupervised voting is by nature more difficult to provide in a secure environment since the voting environment is not controlled by the election administrators' [Xenakis, Macintosh 2004: 3]. The security of e-voting is also influenced by the delivery of multiple channel simultaneous electronic voting. One of the main areas of implementation of e-voting is its legality – so the legal provisions, legal requirements surrounding elections also affect electronic voting's security. Finally, security of e-voting system is also dependent on its usability [Xenakis, Macintosh 2004: 2–4; Fairweather, Rogerson 2002].

Abdalla Al-Ameen and Samani Talab refer to several threats that may pose problems to establishing electronic voting security:

- denial of service, when hackers may compromise the availability to a voting system ("Ping of Death" or "Packet Flooding");
- viruses aiming at destroying e-voting systems;
- worms that are viruses that do not change any existing program or file to spread itself;
- Trojan horses that may be harmless, by deleting or modifying important files from the computer, by planting a harmful virus, or even stealing user's passwords
- physical attacks can also be carried out on e-voting system to sabotage an election [Al-Ameen, Talab 2013: 399–400].

The discussion about introduction of e-voting leads to analysis of motives and potential benefits for the three most important groups of 'beneficiaries' of the tool: voters, public administration and politicians [Krimmer 2010].

From the perspective of the voters, the greatest advantage of electronic voting is the improvement of mobility. The electronic system of voting allows casting a vote at any place and any time (within a time frame specified by law) – even if the voter stays outside his/her place of residence. What is more, modern technologies increase the comfort of voting – the voter no longer needs to leave his/her home in order to reach the polling station. Electronic voting (particularly Internet voting) is also advantageous for disabled people who often have difficulties with getting to a polling station. Thanks to e-voting, people with recognized disability no longer

need to make efforts in order to e.g. organize a means of transport to the polling station. If they have an access to a computer with the Internet connection, they can participate in elections without even leaving their place of residence.

As far as the public administration is concerned, electronic voting can increase the pace and accuracy of counting votes cast during a referendum or an election. This is particularly important because the probability of a mistake made by election clerks is eliminated. Moreover, implementation of an electronic register of voters may eliminate occasional instances of casting multiple votes by a single voter. In countries where e-voting (e.g. the RIV system) has not yet been introduced, a central electronic register of voters can be the first stage of i-voting implementation [Rakowska, Rulka 2011: 14].

E-voting based on the central electronic register of voters can contribute to reduction of costs related to organization of elections and referenda. This argument can be substantiated with the fact that e-voting does not require participation of a large number of election clerks who are indispensable in case of traditional elections taking place at ballot boxes. As far as costs of implementing e-voting are concerned, it was already mentioned that the development, preparation and implementation of the electronic voting system imply relatively high costs in a short period of time. However, as the supporters of e-voting claim, the incurred costs will distribute over a long-term perspective.

Politicians notice the advantages of e-voting systems as well. It is all about changing an image of particular politicians or political parties. Those politicians who support technological progress and introduction of novelties aimed at making various procedures simpler for the citizens are often regarded as more open, friendly and innovative. In such a way, political parties are able to direct their activities in order to expand the electorate, e.g. with the youngest voters. Apart from that, politicians perfectly know that electronic voting systems translate into quicker access to information about election winners and, consequently, into chances to make a coalition in a quicker way, etc. What is more, politicians know that e-voting can increase voting turnouts which directly impact distribution of seats in a parliament. Greater turnout may improve a result of one party, and it can be disadvantageous for the other [Krimmer 2010].

To sum up, it is worth noticing that implementation of ICT into voting procedures can help overcome difficulties linked to polling station being remote from voters, and it can bring about many favorable changes for public administration and politicians who seem to know that e-voting may be a way to convince electorate. That is why it is common to hear that application of new methods for exercising democratic power (particularly during a voting process) is indeed a revolution.

Introduction of new forms of democratic procedures triggers off a discussion about the weaknesses of e-voting. Although modern technologies are commonly applied within trade, business, administration or science, some politicians, experts and scientists are still dubious when it comes to implementation of information and tele-

communication technologies into voting processes. It is substantiated by e.g. the fact that many states expressed their anxieties about mass electoral frauds which might occur during electronic voting. Such uncertainties resulted e.g. from the analyses of the so-called *Zetter Report* (Kim Zetter is a journalist of the "Wired" magazine), who following elections of 2006 has filed a motion to the American electoral commission asking for information about specific problems which occurred during the elections. Zetter has identified over 150 instances of reporting specific problems only within the Sarasota County in Florida. The *Zetter Report* "includes very detailed information about e.g. serial numbers of specific voting computers, last names of the member of electoral commissions, problem description and – what is significant – number of votes lost due to a failure. The report implies that failures of voting computers happened quite often and resulted in loss of votes and registration of invalid votes" [which clearly affected the election result] (…). Apart from the typical "computer" problems, voters reported a series of problems which concerned the fairness of voting: a voter voted on candidate A, yet the computer presented candidate B in the summary screen; regardless of the vote, only candidate A was shown in the summary screen; the summary screen reported the vote as invalid (no candidate selected) despite the voter claimed to choose candidate A or B" [Krawczyk 2007b].

Another problem is connected with the transparency of election process [Gerlach, Gasser 2009: 5]. E-voting method is sometimes called a "black box" due to the fact that the voters, candidates and even officials do not really know how the voting machines operate, and only a small group of specialists (system administrator) and other experts have the notion of the technical aspects of voting and the manner of vote counting. It should be mentioned here that such doubts are, to a large extent, based on experiences – e.g. Great Britain where on 29 January 2007, a report on the British pilot electronic voting conducted in England, Wales and Scotland until 2000 was published [Krawczyk 2007a]. In the electoral commission report the risks associated with e-voting were defined as "considerable and unacceptable" [*May 2007 pilot scheme*] and ceasing of the pilot project until developing a coherent strategy specifying the potential benefits of such voting was simultaneously recommended [Murdoch 2007].

In addition, a very crucial argument against electronic voting is the concern that e-voting may divide the society into two parts: those who have access to the Internet and those who do not use it – mainly because of lack of access. This, in turn, may result in emerging of a "digital gap" (*digital divide*) [Norris 2001] and constitute a serious problem which will cause more social disproportions in many geographical regions.

Another crucial problem concerns identification of the voters. On the one hand, a password and electronic signature should be considered helpful at the stage of voting. On the other hand, one needs to be aware of the fact that such data may not be necessarily used by the voter to which it has been assigned. Moreover, the electronic voting systems are susceptible to many technical problems. Votes based on ICT may

be susceptible to attacks (e.g. from personal computers) which may eventually lead to significant disruption of the voting process. Thus, the servers, systems, computers and voting kiosks should be protected enough to disallow any hacks and infections with computer viruses.

The issue of security features within electronic voting systems is addressed by Michał Rajkowski [2010], who directs attention to dozens of such important elements of his selection:

- privacy – the cast vote has to remain confidential to guarantee that voters express their will without fear of being intimidated;
- accuracy – election results have to reflect the choice of voter in a precise way;
- receipt-freeness – denotes inability of a voter to receive/create a receipt which indicates the voting method; this feature aims at protecting against trade of votes;
- *eligibility* – only eligible voters have the right to vote, any votes cast by non-eligible voters are not taken into consideration;
- un-reusability – each eligible voter is entitled to cast only one correct vote, which would guarantee that each voter has the same (partial) influence on the final result of voting;
- fairness – no partial election results are presented before the elections are officially closed;
- robustness – the system remains secure, even in case of any errors/disruptions (yet of a limited scope) regardless of their source (voter, system administrator, external factors);
- completeness – all correctly cast votes have to be correctly counted;
- soundness – resistance to errors/disruptions – an example is the system protection which disallows a dishonest voter from cancelling the voting process;
- inalterability – once a vote has been cast by the voter, neither the voter nor anyone else (both from within the system and outside it) will be able to change it;
- personal verifiability – it must be possible to verify if the voting result is correct and whether an unauthorized person could have an impact on it during elections; the voter must have possibility to verify whether the vote has been properly cast;
- universal verifiability – similarly to the above case, with the only difference that everyone can verify correctness of the votes;
- dispute-freeness – the fact that voting participants (voters/administration) act in accordance with the voting protocol may be publicly confirmed (during any phase of elections) by any person (from and beyond the system);
- incoercibility – there must not be a possibility to coerce into casting a vote against the will or convictions of an eligible voter.

As regards weaknesses of e-voting and various devices applied in voting, it should be noticed that there may appear the following difficulties when using voting machines (voting computers):

– firstly, undefined security level of voting computers (…) mainly based on operating systems of general application (e.g. *Microsoft Windows*) and specialist software and not subject to independent security certification as per recognized standards (*Common Criteria*), which does not guarantee fairness of voting;
– secondly, problems with initiating the computers and their stability, which with strictly scheduled duration of elections may result in lack of possibility to cast votes by part of voters (such problems occurred among others during the American elections in 2006);
– thirdly, the elevated costs of purchasing voting machines (which is particularly crucial within the opening period of e-voting implementation).
– In comparison with the traditional method of voting (on a ballot paper in a polling station), costs of such e-voting are very high. As Piotr Krawczyk emphasizes, this cost is particularly noticeable when it is "necessary to buy several computers per one commission and at a low level of depreciation (used every few years including costs of storage during this period)" [Krawczyk 2007b].

In case of Internet voting, however, problems of different nature become apparent. We should mention here particularly:

– the need to guarantee unambiguous confirmation of identity, e.g. using the qualified signature. This is certainly connected with less availability of such election procedure due to scarce popularity of this manner of confirming an identity as well as due to a high cost of implementing such solution;
– "lack of a guarantee to stay anonymous, which is contrary to the requirement for strong authentication (only the central system conducts vote anonymisation, but is remains beyond control of the voter – unlike the unsigned ballot paper)" [Krawczyk 2007b].

It is also worth mentioning that voting on voting machines as well as online voting decrease transparency and auditability of election procedure. This results from the fact that members of the electoral commission and (…) do not have a direct view into the process of vote counting which is held within the system constituting, in their opinion, the "black box". In order to minimize those problems, it is often advocated to apply a combination of various *e-voting* systems that allow for counting votes electronically with a paper receipt of the vote (e.g. *Punchscan*) as well as systems which employ cryptographic techniques. They are not, however, the solution for all the problems [Krawczyk 2007c, 2007b].

In the analysis of literature devoted to electronic voting, the most common weaknesses of *e-voting* can be indicated. They often include doubts about ensuring security of procedures on various stages of elections. We should mention here e.g.:

- lack of transparency;
- limited openness and understanding of the system among the non-specialists;
- lack of developed standards for e-voting systems;
- possibility of contravening secrecy of voting, particularly within systems that both authenticate the voters and handle the voting;

- the risk of manipulation by the so-called 'insiders' (system administrators) who have broader access to the system, or by external hackers;
- increased costs of purchase and maintenance of the e-voting system;
- higher security requirements concerning protection of the voting system during and between elections, including the time of transport, storage and maintenance;
- decreased supervision of the election administration;
- limiting the need to re-count the votes;
- the need to conduct additional campaigns to educate the voters;
- possible conflict with currently applicable rules of law;
- possible distrust among the voters to participate in electronic elections, which is the consequence of weaknesses referred to above [*Introducing Electronic Voting*... 2011: 8–9].

Analysis of motives for introducing electronic voting in many states of Europe and the world shows that most of arguments tend to be repeated in various discussions. The most common motives include: increasing mobility of voters, greater availability of the voting for people residing beyond borders of the country, increasing voter turnout by providing an additional voting platform, broadening access to democratic platform for elder, sick and disabled citizens, decreasing voting costs, publishing voting results in a quicker and more independent way [Remmert 2004: 13–16].

Taking into account just some of the arguments of e-voting opponents, many states (despite great interest in this form of electoral participation) abandoned e-voting implementation claiming that e.g. it is too risky to guarantee correctly held elections. Other states tend to disregard advantages of electronic voting in comparison with traditional form of casting votes, or they claim that the range of Internet infrastructure disallows implementation of similar solutions.

CONCLUSIONS

As far as the influence of new information and communication technologies on political life is concerned, it should be remembered that application of ICT allows one of the most appreciated advantages: to remove barriers connected with actual remoteness between the voters and those who exercise power or represent them. That is why it is common to hear that application of new methods for exercising democratic power is indeed a significant change of quality. One of the most important tools of electronic democracy is e-voting which becomes increasingly more popular in various parts of the globe and manifests itself in greater number of pilot projects and initiatives aiming at introducing e-voting into the electoral procedures. Today – in face of rapid civilization progress related also to the IT revolution – the popularity of electronic voting increases.

E-voting, which is already very popular in some states (e.g. Estonia, Switzerland, etc.), manifests itself in greater number of pilot projects and initiatives.

One should notice that despite the positive trend toward e-voting, governments in many countries still display reluctance to implement such an electronic tool of civic participation. These attitudes result mainly from the fact that many opponents of applying electronic tools to democratic procedures consider e-voting as dangerous for political system arguing it is impossible to guarantee its security and ensure fulfilling democratic principles, e.g. secrecy or universality of the voting [Musiał-Karg 2014: 315].

Despite ongoing technical problems with e.g. ensuring safety of elections, multiple advantages (for various groups: voters, politicians, public administration) as well as positive experiences of many countries can constitute a considerable stimulus for implementing e-voting in Europe as well as in other countries of the world.

However, during discussions about implementation of e-voting, the government and officials should take into account the weaknesses of e-voting connected mostly with security of the casting procedure as well as the security of vote counting in elections and referenda. Thus, following the opinion of the Internet Society Poland, it is worth noticing that "constant and necessary conditions which apply to any future changes to election procedures should include: anonymity, secrecy, impossibility to trade votes, correctness of the results and verifiability for the voters" [*Statement of the Internet Society…* 2007].

Despite difficulties with e-voting that have been referred to above, the number of states interested in implementation of this solution is constantly increasing. Good practices of e.g. Estonia and Switzerland (where e-voting systems have been introduced), surely will function as examples for states that plan to introduce this alternative manner of participation in elections. During implementation of e-voting systems, it should be remembered to take advantage both of the good as well as the difficult experiences, current state of knowledge and threats indicated by scholars within this scope.

BIBLIOGRAPHY

A Comparative Assessment of Electronic Voting, http://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=description&lang=e#fg1 (access 11.06.2015).

Al-Ameen, A., Talab, S. 2013. *The Technical Feasibility and Security of E-Voting*, "The International Arab Journal of Information Technology", Vol. 10, No. 4, pp. 397–404.

Fairweather, B., Rogerson, S. 2002. *Technical Options Report*, De Montfort University, Leicester.

Gerlach, J., Gasser, U. 2009. *Three Case Studies from Switzerland: E-Voting*, "Berkman Center Research Publication", no. 03.1.

Goldsmith, B., Ruthrauff, H. 2013. *Implementing and Overseeing Electronic Voting and Counting Technologies*, International Foundation for Electoral Systems and National Democratic Institute for International Affairs, Washington D.C.

Introducing Electronic Voting: Essential Considerations, [in:] "Policy Paper", International Institute for Democracy and Electoral Assistance, December 2011, pp. 8–9.

Krawczyk, P. 2007a. *Brytyjski raport o e-votingu*, IPsec.pl, http://ipsec.pl/brytyjski-raport-o-e-votingu.html (access 10.05.2015).

Krawczyk, P. 2007b. *E-voting: omówienie raportu Zettera*, IPsec.pl, http://ipsec.pl/e-voting%3A-om%C3%B3wienie-raportu-zettera.html (access 10.05.2015).

Krawczyk, P. 2007c. *Nowości w e-votingu*. SecurityStandard.pl. Kravietz. The blog of Paweł Krawczyk about IT security, http://blog.securitystandard.pl/news/118832.html (access 13.08.2014).

Krimmer, R. 2010. *E-Voting in Austria. Current Status in and around Austria*, March 11, IECEG Conference, Belek, Turkey.

Mägi, T. 2007. *Practical Security Analysis of E-voting Systems* (Master Thesis), Tallin, http://www.cs.nccu.edu.tw/~raylin/MasterCourse/SelectedTopicsIS/Spring2009/master%20thesis%20e-voting%20security.pdf (access 14.06.2015).

May 2007 pilot scheme. The Electoral Commission, http://www.electoralcommission.org.uk/elections/modernising_elections/May2007 (access 19.03.2014).

Moynihan, D. P. 2004. *Building Secure Elections: E-Voting, Security, and Systems Theory*, "Public Administration Review", Vol. 64, No. 5, pp. 515–528.

Murdoch, S. J. 2007. *Electoral Commission releases e-voting and e-counting reports,* Light Blue Touchpaper, http://www.lightbluetouchpaper.org/2007/08/02/electoral-commission-releases-e-voting-and-e-counting-reports/ (access 15.03.2015).

Musiał-Karg, M. 2014. *Electronic Voting. Selected issues concerning implementation of a new tool of civic democratic participation,* [in:] *EIIC 2014. The 3rd Electronic International Interdisciplinary Conference, Proceedings in Electronic International Interdisciplinary Conference*, M. Mokryš, S. Badura, A. Lieskovsky, (eds.), EDIS – Publishing Institution of the University of Zilina, Slovakia.

Musiał-Karg, M. 2012. *Elektroniczne referendum w Szwajcarii. Wybrane kierunki zmian helweckiej demokracji bezpośredniej*, WNPiD UAM, Poznań.

Musiał-Karg, M. 2011a. *Internetowe głosowanie w E-stonii na przykładzie wyborów w latach 2005–2009*, "Przegląd Politologiczny", no. 3, pp. 99–117.

Norris, P. 2011. *Digital Divide. Civic Engagement, Information Poverty, and the Internet Worldwide,* Cambridge.

Nowina-Konopka, M., *Elektroniczna urna*, http://www.rpo.gov.pl/pliki/12066058070.pdf (access 15.06.2015).

Pieters, W. 2006. *Acceptance of Voting Technology: between Confidence and Trust?*, [in:] *iTrust*, K. Stølen et al. (eds.), Springer-Verlag Berlin Heidelberg.

Rajkowski, M. 2010. *System głosowania elektronicznego*, http://cygnus.tele.pw.edu.pl/~zkotulsk/seminarium/System_glosowania.pdf (access 14.03.2015).

Rakowska, A., Rulka, M. 2011. *Centralny elektroniczny rejestr wyborców podstawą reform prawa wyborczego*, The Institute of Public Affairs, Warsaw.

Remmert, M. 2004. *Towards European Standards on Electronic Voting,* [in:] *Proceedings of the 1st ESF TED Workshop on Electronic Voting,* A. Prosser, R. Krimmer (eds.), GI LNI P-47, Bregenz.

Statement of the Internet Society Poland (ISOC) concerning e-voting in general elections, adopted by the ISOC Management Board on 10th January 2007 (resolution of the ISOC Poland Management Board no. 2/2007), Internet Society Poland, http://www.isoc.org.pl/200701/wybory (access 13.06.2015).

The Carter Center Handbook on Observing Electronic Voting. 2012. The Carter Center, Atlanta.

Weldemariam, K., Villafiorita, A., Mattioli, A. 2007. *Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach*, [in:] *E-Voting and Identity*. First International Conference VOTE-ID 2007, A. Alkassar and M. Volkamer (eds.), Springer-Verlag Berlin, Heidelberg.

Xenakis, A., Macintosh, A. 2004. *Procedural Security of Electronic Voting*, [in:] *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.5608&rep=rep1&type=pdf (access 15.09.2015).

ABOUT THE AUTHOR

Magdalena Musiał-Karg, works at the positon of Professor at the Department of Political Systems of Faculty of Political Science and Journalism at the Adam Mickiewicz University in Poznań. She specializes in the fields connected with direct democracy and implementation of modern technologies into voting processes (e-voting). The author's scholarly and research interests focus also on the issues connected with the political participation, role of women in politics and transborder cooperation on the borderline of Poland and Germany. Coordinator of the Research Group "Helvetic Initiative" (http://helwecja.amu.edu.pl/).