Voting in E-Participation: A Set of Requirements to Support Accountability and Trust by Electoral Committees

Peter Parycek[1], Michael Sachs[1], Shefali Virkar[1(✉)], and Robert Krimmer[2]

[1] Department for E-Governance in Administration, Danube University Krems, Krems an der Donau, Austria
{peter.parycek, michael.sachs, shefali.virkar}@donau-uni.ac.at

[2] Ragnar Nurkse Department for Innovation and Governance, Tallinn University of Technology, Tallinn, Estonia
robert.krimmer@ttu.ee

Abstract. Voting is an important part of electronic participation whenever it comes to finding a common opinion among the many participants. The impact of the voting result on the outcome of the e-participation process might differ a lot as voting can relate to approving, polling or co-decision making. The greater the impact of the electronic voting on the outcomes of the e-participation process, the more important become the regulations and technologies that stipulate the voting system and its procedures. People need to have trust in the voting system in order to accept the outcomes. Hence, it is important to use thoroughly trustworthy, auditable and secure voting systems in e-participation; especially whenever the voting within the e-participation process is likely to have a significant impact on the outcome. This paper analyses the verdict of the Austrian Constitutional Court in relation to the repeal of the Elections to the Austrian Federation of Students in 2009 where electronic voting was piloted as additional remote channel for casting a ballot. The court states its perspectives on elections and electronic voting which serve as sources for the derivation of legal requirements for electronic voting in this paper, namely requirements for accountability and trust by the electoral committee. Then, possible solutions for the requirements based on scholarly literature are described. The paper does not intend to explicitly provide e-voting solutions for elections, but instead proposes to serve as a basis for discussion of electronic voting in different e-participation scenarios.

Keywords: E-participation · E-voting · Electoral committee · Accountability · Trust

1 Introduction

Electronic participation is characterized by the participation of citizens in political decision-making processes with tools based on modern information and communication technologies (ICTs). Procedures for the participation of citizens in the decision-making

R. Krimmer et al. (Eds.): E-Vote-ID 2017, LNCS 10615, pp. 42–56, 2017.
DOI: 10.1007/978-3-319-68687-5_3

process are possible at all administrative levels, from the municipality to the European Union, but can also be integrated in other contexts such as private organisations. The implementation of electronic participation has the potential to reduce hurdles for participation and to lower the costs of these processes in the long-term [1].

E-participation can be used for various purposes and in different forms, hence, the processes and platforms are often tailor-made for specific contexts. Models that describe e-participation usually divide elements of participation according to the degree of impact each has on the final decision [2]. While low levels of participation, such as accessing information or commenting on ideas, do usually not require strong regulations and high technical security standards, forms of participation with high impact on decision-making outcomes require the implementation of higher standards. As soon as selections and votes are part of the participation process, technical security and detailed regulations are required in order to establish trust in the outcomes of the participatory actions. The greater the impact of the participatory process on the final result, the higher the demands for proper regulations, implementation and secure systems [3].

E-voting in its legally binding context of official elections is the form of e-participation with the most direct impact on the actual decision. Consequently, it is relevant to look closely at e-voting requirements for use in secure voting processes in e-participation.

1.1 Background: The Elections to the Austrian Federation of Students

The elections to the Austrian Federation of Students in 2009 have been the first and only instance of electronic voting in Austria up until now. As the level of participation is traditionally low in the elections to the Austrian Federation of Students [4], e-voting was seen as a means with the potential to increase engagement and to test new technology within a young target group. The implementation of an e-voting pilot as additional remote channel to cast a vote along side the paper ballot in these elections was accompanied by a controversial discussion among students and in the public.

The update of the Regulation of the Elections to the Austrian Federation of Students from 2005[1] came into effect on 3 October 2008 and expired on 13 January 2012. The regulation was challenged by individuals in the Austrian Constitutional Court, which repealed the regulation on e-voting as it was not in alignment with the corresponding Federation of Students law. Consequently, the election was considered invalid. Major issues influencing the verdict of the Constitutional Court pertained to regulations related to the electoral committee and a lack of clear definitions concerning the processes of the verification within the entire voting system. For a comprehensive analysis, see the works of Krimmer, Ehringfeld and Traxl [5, 6].

[1] In German: "Hochschülerinnen- und Hochschülerschaftswahlordnung 2005". Available at: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR30006701.

1.2 Relevance for the Electoral Committees and Accountability

The Austrian Constitutional Court dealt extensively with the Austrian Federation of Students elections in 2009, and the relevant judgements can provide guidelines for the implementation of secure e-voting in any context. This paper aims, therefore, to provide a basis for the discussion of possible solutions to legal and technical issues encountered during the adoption of an e-voting system based on the demands made by the Constitutional Court.

In the framework of electronic participation, participatory decision making is usually not legally binding. E-voting regulations for officially binding elections hence address the highest standards of *security*, *audibility* and *reliability*, and are of relevance within the context of co-decision making in e-participation.

One must bear in mind that voting regulations and suffrage differ among countries, and even differ within countries depending on the purpose and context of the voting process. While the requirements formulated in this document may not be directly applicable to different electronic voting contexts they do indeed serve as a base for the creation of tailor-made solutions.

1.3 Structure of the Paper

In order to provide a robust analysis of e-voting as a participatory mechanism, and to present an informed account of the legal concepts and technical solutions underpinning the requirements for secure electronic voting in Austria, this research paper is structured as follows. First, the chapter entitled *Methodology* presents an account of the research design and methodological tools employed by the authors within the context of this research project. The next chapter, *Requirements based on Literature*, examines the selected legal requirements as embedded case studies supported by evidence based in scholarly and practitioner literature. The penultimate chapter, *Discussion*, offers an informed concluding analysis of e-voting and its potential as a tool for greater public engagement; locating the process within the broader conceptual framework of e-participation in Europe. The paper closes with the final chapter, *Acknowledgements*.

2 Methodology

This paper takes into account the legal considerations of the Austrian Constitutional Court ruling regarding the implementation of e-voting in the Elections of the Austrian Federation of Students of 2009 in order to reflect the requirements for secure voting systems that enable the electronic participation of citizens. For this purpose, legal requirements for electronic voting were derived from the verdicts passed by the Austrian Constitutional Court. Possible solutions for these requirements were then extracted in a literature analysis of international scientific works. While the original study takes into consideration all requirements derived from the judgements of the Austrian Constitutional Court, this paper focuses on those that consider the requirements for the electoral committee and those that pertain to system accountability as

these can potentially be transferred to other scenarios and contexts of voting as a form of e-participation.

2.1 Deduction of Requirements

Sentences of the Austrian Constitutional Court were analysed for references to e-voting in the Elections of the Austrian Student. Not all judgements with such references included relevant information, for some appeals were rejected as they were not considered lawful or valid. The source of the sentences was the website of the Legal Information System of the Republic of Austria.[2] The following pronouncements of the Constitutional Court were analysed, and they are listed below according to date of sentence and reference number:

- 25 June 2009, V28/09, V29/09 ua
- 10 December 2009, G165/09, V39/09
- 23 February 2010, V89/09
- 9 March 2011, G287/09
- 02 December 2011, WI-1/11, V85/11ua, B1214/10, B1149/10, B898/10
- 5 March 2012, WI-2/11
- 22 August 2014, WI 2/2014

Once all possible legal requirements were extracted from the original texts they were clustered and filtered. These requirements were then further simplified for the purpose of better handling, and redundant requirements were merged with others or deleted. The categories for the clustering were thereafter derived from the content of all requirements and not prior based on literature. In this paper the authors only discuss the requirements that are part of the categories *electoral committee* and *accountability*.

2.2 Literature Research for Solutions

This section consists of a description of the research strategy adopted by the authors whilst conducting a review of existing literature for legal concepts and technological solutions relevant to the research project. To search for literature pertaining to electronic voting in general and to the derived legal requirements in particular, this project made use of one database of peer-reviewed literature (Scopus), one specialist search engine (Google Scholar), and one database of full-text books (Google Books).

The *Scopus Database* was queried specifically for peer-reviewed, scholarly literature. In order to optimally utilize the resource, a systematic conventional query string was constructed to conduct the search within the 'title', 'abstract' and 'keywords' fields of the publications indexed by this database. Searches were also filtered by scholarly discipline in order to narrow down search results and to identify highly relevant material. This research project also made use of the *Google Scholar* search engine to recover full-text sources of material previously discovered using Scopus, to identify clusters of publications authored by the same person, and to obtain new citations

[2] https://www.ris.bka.gv.at/defaultEn.aspx.

through a conventional key word search. The *Google Books* database was also queried exhaustively in order to access material from both single-author books and chapters within edited volumes. Here, books identified from earlier literature searches were first looked up, either by publication name or by author/editor name or a combination of the two. A conventional keyword search was also pursued.

3 Requirements Based on Literature

This chapter outlines and analyses the legal requirements for the implementation of secure e-voting in Austria derived from the rulings of the Austrian Constitutional Court. In particular, it discusses in some detail an extensive collection of legal concepts and technical solutions extracted through a systematic literature analysis of international scientific works that are considered relevant to the two sets of legal requirements selected as the embedded case studies for this research paper.

The research findings presented are organised in the following manner: first, the chapter comprises of three sections. The first section presents the derivation of the requirements based on judgements passed in Austria by the Constitutional Court, and introduces the embedded case studies. The second section is then concerned with derived legal requirements for the electoral committee, and the third with derived legal requirements pertaining to electoral accountability. Each stipulated legal requirement is listed individually, and is followed immediately by a discussion that touches upon how existing scholarly literature informs the legal condition conceptually and/or where developments in technology further reflect or advance key fundamental legal concepts.

As this paper does not seek to provide concrete solutions for electronic distance voting, but guidelines for voting at different stages within e-participation processes, literature about remote electronic voting and electronic voting machines was considered for the scholarly discussion below.

3.1 Legal Requirements at a Glance: The Embedded Case Studies

The analysis of the verdicts passed by the Austrian Constitutional Court yielded at total of 28 legal requirements, grouped by these researchers within 5 categories. Of these 5 categories, two – *electoral committee* and *accountability* – were selected as embedded case studies for this research paper.

Out of the 28 requirements identified, 5 relate to the category *electoral committee*. The derived requirements for the category *electoral committee* include that: the electoral committee must be able to carry out all its statutory tasks; the electoral committee must accept/receive the ballot; the electoral committee must examine the electoral authority/eligibility of the elector; the verification of the identity of the person entitled to vote must take place before the transmission of the electoral form; and, a certification of the e-voting system by experts cannot replace the state guarantee of the electoral principles observed by electoral committees.

Another 5 derived requirements may be clustered around the category *accountability*. These include: the electoral committee must be able to determine the election results and their validity; the verification of the validity of the ballot papers must be

ensured by the electoral committee; the electoral committee and the judicial authorities of public law must be able to carry out a verification of the electoral principles and results after the election; the essential steps of the electoral process must be reliably verified by the electoral committee (without the assistance of experts) and the judicial authorities of public law; and, the essential steps of the determination of results must be reliably verified by the electoral committee (without the participation of experts).

3.2 Requirements for Trust by Electoral Committees

This section discusses the legal concepts and technical solutions pertaining to the requirements for trust by electoral committees as identified in the scholarly and practitioner literature.

The electoral committee must be able to carry out all its statutory tasks. Today, a large percentage of electoral management bodies (EMBs) use information and communications technologies with the aim of improving administrative procedures associated with the electoral process [7]. Technologies deployed range from the use of basic office automation tools such as word processing and spreadsheets to the application of more sophisticated data processing tools including data base management systems, optical scanning, and geographic information systems [8].

According to Caarls (2010), for an EMB to successfully carry out all its statutory tasks, therefore, it is important that a two-pronged approach be adopted [9]. On the one hand, the tasks and responsibilities of the EMB need to be defined clearly in legislation [10]. The extent to which the EMB is involved with the electoral process has direct bearing on the type and nature of the technological solution it deploys. On the other, it is also vital that personnel within the EMB possess the necessary technical expertise to effectively manage the process of electronic voting [11]. Only when both pre-conditions are fulfilled will the administering electoral body be able to successfully adopt and implement technology solutions to effectively perform and enhance its functions. For technical solutions see also (amongst others) Prosser et al. (2004) [12].

The electoral committee must accept/receive the ballot. Remote electronic voting refers to the election process whereby electors can opt to cast their votes over the Internet, most usually via a Web browser from home, or from possibly any other location where they have Internet access [13]. Whilst many different aspects of this sort of election warrant closer accountability, the focus of this recommendation is on *security*.

Voting in the traditional way, according to Chiang (2009), with physical ballots submitted at a true polling station, is usually done with confidence because the tangible safeguards put in place ensure a tangible return to the electoral management authority [14]. Technology-enabled elections are viewed with suspicion as votes might be intercepted and tampered with at the time of transmission to the electoral authority servers [15].

Just as the revamped election system needs to be seen as both *reliable* and *trustworthy* by electors [16], so must the system be considered impenetrable to external malicious attacks or intent by the administering authority says Pieters (2006). In recognising this, Andreu Riera Jorba and Jordi Castella Roca have developed and

patented under United States law a secure electronic voting system that employs interrelated cryptographic processes and protocols to provide reliability to vote casting, ballot recounts, and verification of vote or poll results [17].

The electoral committee must examine the electoral authority/eligibility of the elector. Within the European Union, Ikonomopoulos et al. (2002) have determined that the process of examining the electoral authority/eligibility of the elector is a two-fold procedure. First, the process of determining electors is performed, a step essential for the current voting process, wherein all persons above a certain age have either the right or the obligation to participate in the democratic process [18]. This stage is realised by the state employees working for the electoral authority who determine, according to the national census, each individual's age and legal status. Second, the requirement of providing a means of authentication to each elector then needs to be fulfilled. This is achieved when state employees create a means of identification for every elector, and when these are subsequently received by voters from the state.

Therefore, for an electronic voting system to be at once *secure*, *legitimate* and *complete*, Ikonomopoulos et al. (2002) hold that it is important for the electoral committee be able to determine and establish the electoral authority/eligibility of the elector from a (1) legal, (2) functional, and (3) security systems-requirement perspective. The legal framework for the traditional model of voting advanced above provides us with a basis for the e-voting system requirements specification. In terms of functional requirements, the starting point of any of interaction with the information system is thus the provision of access to system functions that each actor is authorised to perform [18]. Building on this, Ibrahim et al. (2003) have proposed a secure e-voting systems architecture that applies security mechanisms in order to meet the legal security requirements needed for any election process. According to the proposed system, as individuals register themselves with the administrator of e-voting to be counted amongst eligible voters, a validator is made responsible for the verification of elector authority/eligibility and for the production of a ballot ID [19].

The verification of the identity of the person entitled to vote must take place before the transmission of the electoral form. In traditional voting/balloting, the authentication of an elector is generally performed prior to the act of electing, when the elector appears in person to vote at the election centre where they are registered [18]. Ikonomopoulos et al. (2002) outline the process in some detail; wherein the voter arrives at the polling station, presents to the on-duty member of staff his or her identity papers, has them verified by the staffer in question, and is then presented with the current electoral ballot paper. This process is performed to ensure that the elector themselves votes, and consists of an interaction between the elector and the electoral authority as represented by the personnel at the election centre [18].

For Internet voting to be secure, according to Regenscheid et al. (2011), a similar procedural requirement has often to be met: that the identity of the eligible elector needs to be verified prior to the electronic transmission of the electoral form. In the United States of America, for instance, state and local jurisdictions are given the option to employ systems to authenticate Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) voters before serving them electoral forms, when permitted under state law [20]. However, if voter identification data is indeed used to establish trust that

a given ballot was completed and returned by an eligible elector, it is carried out on the premise that the electronic authentication of the person entitled to vote was done prior to any transmission of the electronic ballot form [20].

A certification of the e-voting system by experts cannot replace the state guarantee of the electoral principles observed by electoral committees. Richter (2010) states that "…all forms of voting, including Internet voting have been criticized for not fulfilling the Principle of the Public Nature of the Election which was declared as a constitutional principle in the Voting-Machine-Judgement of the German Federal Constitutional Court (BVerfG09) and which requires verifiability of the election for every citizen without technical knowledge" [21].

According to Gritzalis (2002), electronic voting should be considered only as a complementary means to traditional election processes [22]. He argues that while e-voting can be a cost-effective way to conduct the electoral process and a means of attracting specific groups of people to participate, the continued prevalence of (1) the digital divide within adopting societies, (2) an inherent distrust in the e-voting procedure across populations, and (3) inadequate mechanisms to protect information systems against security risks make it only a supplement to, and not a replacement of, existing paper-based voting systems.

Building on this argument, Caarls (2010) attempts to highlight the issues of trust and confidence as necessary pre-conditions for the uptake of e-voting systems [9]. Here, Caarls argues that an e-voting system cannot be successfully adopted unless citizens trust their current (paper-based) political and administrative systems. Further, she maintains, the introduction of an e-voting system must not result in the exclusion of certain groups within a given population. Security is also paramount, with time needing to be set aside for research into the development of robust and secure system before the eventual roll-out of the project. This is also tightly connected with the topic of verifiability, which will be deal with in the next section.

3.3 Requirements for Accountability

This section considers the legal concepts and technical solutions pertinent to the derived legal requirements for accountability as obtained from the scholarly and practitioner literature.

The electoral committee must be able to determine the election results and their validity. As part of the electoral process, the election authority needs to be able to verify the validity of every ballot cast, and that the tallying of the valid ballots has been correct.

In the electronic voting literature, the term *verifiability* is closely related to the accountability requirement of the integrity of the election result [23]. Gritzalis (2002) contends, therefore, that an e-voting system should allow for its verification by both individual voters (individual verifiability), and also by election officials, parties, and individual observers (institutional or universal verifiability) – despite being in conflict with principles of transparency [22]. Systems providing both types of verification are known as *end-to-end* (E2E) *verifiablility* [24]. However, the ability of currently existing

electronic voting systems to enable the election authority to verify the integrity of the election result has been criticised as being flawed by recent scholarship [25].

This is because, as maintained by Gharadaghy and Volkamer (2010), universal verifiability is usually more complex to achieve than individual verifiability for, in order to attain this condition, the election authority needs to ensure that all encrypted votes cast and stored on the database are decrypted appropriately and properly tallied whilst preserving ballot secrecy [24]. Gharadaghy and Volkamer go on to propose two main cryptographic techniques to meet and overcome this challenge: either (1) the application of homomorphic encryption schemes, such as the *Helios 2.0* protocol [26], that allow the encrypted sum of all encrypted votes to be computed without compromising the secrecy of the ballot; or (2) the use of *MIX networks* to anonymize encrypted votes prior to their decryption and eventual tallying [24]. Further, for a discussion of organisational issues see also Krimmer (2016) [27].

The verification of the validity of the ballot papers must be ensured by the electoral committee. It is the task of the electoral committee to ensure the validity of the each of the ballot papers counted towards the final election result.

The need for reliability of the e-voting process, according to Gritzalis (2002), is derived from the democratic need to ensure that the outcome of the election correctly reflects the voters will [22]. In other words, a reliable system should ensure that the outcome of the voting process accurately corresponds to the votes cast. It should be impossible from a systems architecture point of view to exclude from the tally a valid vote and to include an invalid one [28].

Khaki (2014) proposes both basic and advanced security protocols that may be applied by an electoral management body to successfully verify the validity of the submitted ballot papers [29]. Basic security measures advanced by this author include either the use of Message Authentication Code (MAC) keys shared between the voter and the server, or server digital signatures that constitute keys stored on the server. In both cases, the server is able to generate for verification purposes the MAC or digital signature of any vote.

Further, according to Khaki, vote integrity and authenticity can be assured through the use of advanced security measures in the form of voter digital signatures [28], wherein votes are digitally signed by the voter after they have been encrypted in such a manner that the recipient server can validate and verify the signature as authentic but cannot manipulate it. For an early technical proposal see [30].

The electoral committee and the judicial authorities of public law must be able to carry out a verification of the electoral principles and results after the election. In the post-election period, Caarls (2010) recommends that an audit trail be established for all aspects of the systems used in the elections so that "…all changes and decisions can be explained and defended" [9]. Following from this, therefore, audits may be carried out by all the parties involved in the electoral process and can serve many purposes. To paraphrase Norden et al. (2007), such an audit can fulfil the following goals: (1) create public confidence in the election results, (2) deter election fraud, (3) detect and provide information about large-scale systemic errors, (4) provide feedback towards the improvement of voting technology and election administration, (5) set benchmarks and provide additional incentives for election staff to achieve higher standards of accuracy,

and (6) confirm, to a high degree of confidence, that a complete manual recount would not affect the election outcome [31].

There exist in the practitioner literature three noteworthy e-voting protocols that overtly permit the electoral management body to carry out such a post-election verification of electoral principles and results [32–34].

A. Punchscan: Fisher et al. (2006) in their seminal paper put forward Punchscan, a hybrid paper/electronic voting system based on a concept delineated by David Chaum in December 2005 [32]. In improving upon the earlier idea, the Punchscan system advanced by Fisher et al. employs a two-layer ballot and receipt system in combination with a sophisticated cryptographic vote-tabulation mechanism called a "Punchboard" that can be used to facilitate the running of an electronic election. During the post-election phase, once the results of the ballot are posted online, auditors may conduct a post-election audit by choosing an area of the Punchboard's decrypt table [32]. Any significant corruption of the Punchboard as a consequence of election malpractice is almost certainly detectable.

B. Helios: Adida (2008) discusses the advantages of Helios, a web-based open-audit voting system [33]. Designed to be deliberately simpler than most complete cryptographic voting protocols, Helios focuses on the central precept of "public auditability" – any group can outsource its election to Helios, and the integrity of that election can be verified even if Helios itself is corrupted. To achieve this, the Helios protocol provides users with the option of two verification programmes written in Python: one for verifying a single encrypted vote produced by the ballot preparation system with the "audit" option selected, and another for verifying the shuffling, decryption, and tallying of an entire election [33].

C. Scantegrity: Chaum et al. (2008) propose Scantegrity, a security enhancement for optical scan voting systems [34]. The Scantegrity voting system combines E2E cryptographic ideas with a widely used vote-counting system to provide the end-user with the strong security guarantees of an E2E set-up whilst not interfering with existing procedural requirements such as a paper audit trail or a manual recount. Scantegrity is furthermore universally verifiable, whereby, using special software of their choice, anyone can verify online that the tally was computed correctly from official data [35]. This makes it particularly useful for those electoral management bodies wishing to carry out a post-electoral audit.

The essential steps of the electoral process must be reliably verified by the electoral committee (without the assistance of experts) and the judicial authorities of public law. From general perspective, in cases where an e-voting system has been deployed, Caarls (2010) advocates that every part of the process be audited post-election; including, the electoral voter register and its compilation, together with the processes of voting, counting, archiving, and the destruction of votes [9]. One part of the audit process could be to verify that the systems used for the election were in fact based on source code certified for use prior to the election. Other parts of the audit process might include the review of other documentation, including the functional and technical system design [9].

In more particular terms of system functionality, and to paraphrase Prandini and Ramilli (2012), e-voting systems are generally evaluated in terms of their security, auditability, usability, efficiency, cost, accessibility, and reliability [36]. The principle of *auditability*, most especially, refers to the necessary pre-condition of there being reliable and demonstrably authentic election records [37] against which due process can be accounted for. Software independence is one form of system auditability, enabling the detection and possible correction of election outcome errors caused by malicious software or software bugs [38]. The concept has been defined by Rivest (2008) as follows: "A voting system is software independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome" [39].

In other words, the principle of software independence addresses directly the difficulty of assuring oneself that cast ballots will be recorded accurately in adherence to prevailing election principles and standards by complex and often difficult-to-test software in the case of an all-electronic voting system [39]. For users of software-independent voting systems, therefore, verification of the correctness of the election result is possible without there being any lingering concern that the election result was affected or even determined by a software bug or malicious piece of code [38].

The essential steps of the determination of results must be reliably verified by the electoral committee (without the participation of experts). Similar to the legal principle of the "public nature of elections" in Germany [40], which prescribes that all the essential steps of an election are subject to the possibility of open accountability by general public, it is argued here that (when applied to the use of electronic voting machines in Austria) both legal and technical provision needs be made for the electoral management body to be able to verify independently and reliably the essential steps of voting and the ascertainment of the result post-election without its personnel possessing any prior specialist knowledge.

Considered in terms of e-voting in general, the holding makes the security objective of *election* or *end-to-end verifiability* mandatory [41]. This is because, in contrast to conventional paper-based elections, electronics-based ballots are still much less transparent [42]. It may not be possible to observe all the electronic operations performed on data, programming errors are usually difficult to detect, and attacks on a system by malicious code might go unnoticed [26].

Remote electronic voting systems have to, therefore, also be considered from the perspective of their *usability* [43]. The term 'usability', according to Winkler et al. (2009), is often used to describe the perceived ease of use and usefulness of an information technology system [43]. Several studies point out the importance of undertaking a usability evaluation when validating a new e-voting system [44]. Within the context of the discussion, it may be inferred that a verifiable system should be user-friendly to ensure that its users are able to carry out verification processes with relative ease and speed and independent of external specialists.

4 Discussion

It has been a declared target by the Europe Ministers responsible for e-government to empower citizens through information and communication technologies [45]. Citizens shall receive better and more transparent access to information that shall serve as the basis for stronger involvement in the policy process. Hence, information and communication technologies shall enhance citizen participation. New political movements and ideas all across Europe support the surge of an increasingly connected society towards having a stronger say in political processes. Traditional parties seek to open up to outside opinions, at least during election campaigns. These changes in the political landscape must be supported with the necessary tools.

Citizens' participation in general is a complex field with numerous different approaches being adopted to achieve similar aims. It has become evident that there is no single possible solution to resolve the various obstacles in the path of optimal citizen participation, but it has also become obvious that digital technologies, the internet and its networking connectivity can support the management of citizen participation at most stages of engagement.

This research paper focuses on the voting process as an integral part of electronic participation. Votes are used to assess the opinions of participants on comments or proposals which might not necessarily need highly regulated and secure technological systems. Voting can also be used to make the final decision in an e-participation process that might have direct impact on actual implementations in reality or legal regulations. In the latter example, observing regulations and ensuring system security are essential for successful and satisfactory participation.

This paper describes the legal requirements for e-voting as stipulated by the Austrian Constitutional Court in the context of the Austrian Federation of Students Election of 2009. While the derived requirements are only valid for this specific context, they can be a good indication for the way forward in other scenarios.

Large-scale e-participation will involve electronic voting at some point in the process, and this must be manged and implemented in an appropriate manner. Public authorities need to be ready to answer citizens' questions, and to have in place a strategy to help citizens understand the system and its underlying technology. Trust-building is a vital component of the engineering of participatory processes.

The introduction of e-participation should be considered as means of promoting social inclusion, and care must be taken to ensure that its proliferation does not result in the privileging of certain groups within society (those who can afford regular Internet access, for instance) over others. In theory, the use of technology in citizens' engagement widens access to the democratic process by reaching out to and inviting a greater number of people to participate. However, in practice existing digital and social divides circumscribe who actually participates and, if not deployed sensibly, technology could actually worsen prevailing democratic deficits.

Acknowledgements. The work of Robert Krimmer was supported in parts by the Estonian Research Council project PUT1361 and the Tallinn Univerity of Technology project B42.

References

1. Viborg Andersen, K., Zinner Henriksen, H., Secher, C., Medaglia, R.: Costs of e-participation: the management challenges. Transforming Gov. People Process Policy **1**(1), 29–43 (2007)
2. Arnstein, S.R.: A ladder of citizen participation. J. Am. Inst. Planners **35**(4), 216–224 (1969)
3. Schossböck, J., Rinnerbauer, B., Sachs, M., Wenda, G., Parycek, P.: Identification in e-participation: a multi-dimensional model. Int. J. Electron. Gov. **8**(4), 335–355 (2016)
4. Krimmer, R.: e-Voting.at: Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen. Working Papers on Information Processing and Information Management 05/2002 of the Vienna University of Economics and Business (2002)
5. Krimmer, R., Ehringfeld, A., Traxl, M.: The use of e-voting in the federation of students elections 2009. In: Krimmer, R., Grimm, R. (eds.) Proceedings of the 4th International Conference on Electronic Voting 2010, pp. 33–44, Bonn (2010)
6. Krimmer, R., Ehringfeld, A., Traxl, M.: Evaluierungsbericht. E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009. BMWF, Vienna (2010)
7. Lopez-Pintor, R.: Electoral Management Bodies as Institutions of Governance. Bureau for Development Policy, United Nations Development Programme (2000)
8. ACE Electoral Knowledge Network. Elections and Technology. http://aceproject.org/ace-en/topics/et/onePage. Accessed 21 Apr 2017
9. Caarls, S.: E-voting Handbook: Key Steps in the Implementation of E-enabled Elections. Council of Europe Publishing, Strasbourg (2010)
10. Mozaffar, S., Schedler, A.: The comparative study of electoral governance – introduction. Int. Polit. Sci. Rev. **23**(1), 5–27 (2002)
11. Gillard, S.: Soft-skills and technical expertise of effective project managers. Issues Inf. Sci. Inf. Technol. **6**, 723–729 (2009)
12. Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: Implementation of quorum-based decisions in an election committee. In: Traunmüller, R. (ed.) EGOV 2004. LNCS, vol. 3183, pp. 122–127. Springer, Heidelberg (2004). doi:10.1007/978-3-540-30078-6_21
13. Rubin, A.D.: Security considerations for remote electronic voting. Commun. ACM **45**(12), 39–44 (2002)
14. Chiang, L.: Trust and security in the e-voting system. Electron. Gov. Int. J. **6**(4), 343–360 (2009)
15. Bishop, M., Wagner, D.: Risks of e-voting. Commun. ACM **50**(11), 120 (2007)
16. Pieters, W.: Acceptance of voting technology: between confidence and trust. In: Stølen, K., Winsborough, W.H., Martinelli, F., Massacci, F. (eds.) iTrust 2006. LNCS, vol. 3986, pp. 283–297. Springer, Heidelberg (2006). doi:10.1007/11755593_21
17. Jorba, A.R., Roca, J.C.: Secure remote electronic voting system and cryptographic protocols and computer programs employed. U.S. Patent No. 7,260,552, 21 August 2007
18. Ikonomopoulos, S., Lambrinoudakis, C., Gritzalis, D., Kokolakis, S., Vassiliou, K.: Functional requirements for a secure electronic voting system. In: Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K. (eds.) Security in the Information Society. IAICT, vol. 86, pp. 507–519. Springer, Boston, MA (2002). doi:10.1007/978-0-387-35586-3_40
19. Ibrahim, S., Kamat, M., Salleh, M., Aziz, S.R.A.: Secure E-voting with blind signature. In: Proceedings of 4th National Conference on Telecommunication Technology. NCTT 2003, pp. 193–197. IEEE Publications (2003)
20. Regenscheid, A., Beier, G.: Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters, NISTIR 7711, National Institute of Standards and Technology (NIST) – U.S. Department of Commerce, Gaithersburg, M.D. (2011)

21. Richter, P.: The virtual polling station: transferring the sociocultural effect of poll site elections to remote internet voting. In: Krimmer R., Grimm R. (eds.) Proceedings of the 4th International Conference on Electronic Voting 2010, pp. 79–86. Bonn (2010)
22. Gritzalis, D.A.: Principles and requirements for a secure e-voting system. Comput. Secur. **21**(6), 539–556 (2002)
23. Küsters, R., Truderung, T., Vogt, A.: Accountability: definition and relationship to verifiability. In: Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS 2010), pp. 526–535. ACM, Chicago (2010)
24. Gharadaghy, R., Volkamer, M.: Verifiability in electronic voting - explanations for non security experts. In: Krimmer R., Grimm R. (eds.) Proceedings of the 4th International Conference on Electronic Voting 2010, pp. 151–162. Bonn (2010)
25. Karayumak, F., Olembo, M.M., Kauer, M., Volkamer, M.: Usability analysis of helios-an open source verifiable remote electronic voting system. EVT/WOTE **11**, 5 (2011)
26. Kremer, S., Ryan, M., Smyth, B.: Election verifiability in electronic voting protocols. In: Gritzalis, D.A., Preneel, B., Theoharidou, M. (eds.) Computer Security – ESORICS 2010. LNCS, vol. 6345, pp. 389–404. Springer, Berlin/Heidelberg (2010). doi:10.1007/978-3-642-15497-3_24
27. Krimmer, R.: Verifiability: a new concept challenging or contributing to existing election paradigms? In: Proceedings of the 13th EMB Conference, pp. 102–107, Bucharest (2016)
28. Mitrou, L., Gritzalis, D., Katsikas, S.: Revisiting legal and regulatory requirements for secure e-voting. In: Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K. (eds.) Security in the Information Society. IAICT, vol. 86, pp. 469–480. Springer, Boston, MA (2002). doi:10.1007/978-0-387-35586-3_37
29. Khaki, F.: Implementing End-to-End Verifiable Online Voting for Secure, Transparent and Tamper-Proof Elections. IDC Whitepaper 33 W (2014)
30. Prosser, A., Krimmer, R., Kofler, R., Unger, M.K.: The role of the election commission in electronic voting. In: Proceedings of the 38th Annual Hawaii International Conference on System Sciences. HICSS 2005, pp. 119–119. IEEE (2005)
31. Norden, L., Burstein, A., Hall, J.L., Chen, M.: Post-Election Audits: Restoring Trust in Elections, Report by Brennan Center for Justice at The New York University School of Law and The Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley School of Law (Boalt Hall) (2007)
32. Fisher, K., Carback, R., Sherman, A.T.: Punchscan: introduction and system definition of a high-integrity election system. In: Preproceedings of the 2006 IAVoSS Workshop on Trustworthy Elections, Robinson College (Cambridge, United Kingdom), International Association for Voting System Sciences (2006). [full citation unavailable]
33. Adida, B.H.: Web-based open-audit voting. In: van Oorschot, P.C. (ed.) Proceedings of the 17th Conference on Security Symposium, pp. 335–348. USENIX Association, Berkley (2008)
34. Chaum, D., Essex, A., Carback, R., Sherman, A., Clark, J., Popoveniuc, S., Vora, P.: Scantegrity: end-to-end voter-verifiable optical scan voting. IEEE Secur. Priv. **6**(3), 40–46 (2008)
35. Sherman, A.T., Carback, R., Chaum, D., Clark, J., Essex, A., Herrnson, P.S., Mayberry, T., Popovenuic, S., Rivest, R.L., Shen, E., Sinha, B., Vora, P.: Scantegrity mock election at Takoma Park. In: Krimmer R., Grimm R. (eds.) Proceedings of the 4th International Conference on Electronic Voting 2010, pp. 35–51. Kollen Druck+Verlag GmbH, Bonn (2010)
36. Prandini, M., Ramilli, M.: A model for e-voting systems evaluation based on international standards: definition and experimental validation. Serv. J. **8**(3), 42–72 (2012)

37. Internet Policy Institute: Report of the National Workshop on Internet Voting: Issues and Research Agenda, An Internet Policy Institute Publication (2001)
38. Rivest, R.L., Virza, M.: Software independence revisited. In: Hao, F., Ryan, P.Y.A. (eds.) Real-World Electronic Voting: Design, Analysis and Deployment. CRC Press, Boca Raton (2017). [full citation unavailable]
39. Rivest, R.L.: On the notion of 'software independence' in voting systems. Philos. Trans. Math. Phys. Eng. Sci. **366**(1881), 3759–3767 (2008)
40. German Federal Constitutional Court (Bundesverfassungsgericht): Use of voting computers in 2005 Bundestag election unconstitutional. Press Release No. 19/2009 of 03 March 2009. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html. Accessed 27 Apr 2017
41. Schmidt, A., Heinson, D., Langer, L., Opitz-Talidou, Z., Richter, P., Volkamer, M., Buchmann, J.: Developing a legal framework for remote electronic voting. In: Ryan, P.Y.A., Schoenmakers, B. (eds.) Vote-ID 2009. LNCS, vol. 5767, pp. 92–105. Springer, Heidelberg (2009). doi:10.1007/978-3-642-04135-8_6
42. Enguehard, C.: Transparency in electronic voting: the great challenge. In: IPSA International Political Science Association RC 10 on Electronic Democracy. Conference on "E-democracy - State of the art and future agenda", Jan 2008, Stellenbosch, South Africa, édition électronique (2008)
43. Winckler, M., Bernhaupt, R., Palanque, P., Lundin, D., Leach, K., Ryan, P., Alberdi, E., Strigini, L.: Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter. In: Proceedings of ICE-GOV (2009)
44. Herrnson, P.S., Niemi, R. G., Hanmer, M.J., Bederson, B.B., Conrad, F.G., Traugott, M.: The importance of usability testing of voting systems. In: Electronic Voting Technology Workshop, Vancouver B.C., Canada, 1 August 2006 (2006)
45. Ministerial Declaration on eGovernment. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf. Accessed 7 May 2017