

REVISITING LEGAL AND REGULATORY REQUIREMENTS FOR SECURE E-VOTING

Lilian MITROU¹, Dimitris GRITZALIS², Sokratis KATSIKAS¹

¹ *Dept. of Information and Communication Systems, University of the Aegean
Karlovassi, Samos GR-83200, Greece
e-mail: l.mitrou@primeminister.gr, ska@aegean.gr*

² *Dept. of Informatics, Athens University of Economics and Business
76 Patission Ave., Athens GR-10434, Greece
e-mail: dgrit@aueb.gr*

Abstract: This paper addresses the democracy-oriented legal and constitutional requirements that an electronic voting system has to comply with. Its scope covers every election or decision-making process, which takes place through voting. Due mainly to the digital divide and to current technological limitation, electronic voting cannot be proposed as a universal means of voting but rather as an alternative option, supplemental to traditional voting means. An electronic voting process must be designed in such a way as to guarantee the general, free, equal and secret character of elections. In a democratic context an electronic voting system should respect and ensure attributes and properties such as transparency, verifiability, accountability, security and accuracy. Only then can it foster and promote the participation of the citizens, the legitimacy and the democratic transaction of the election process.

Key words: Security, electronic voting, voting technologies, user requirements, legal requirements, secure information systems.

Acknowledgements: This work has been supported in part by the European Commission, IST Programme, Project *e-vote* (*An Internet-based electronic voting system*).

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35586-3_46](https://doi.org/10.1007/978-0-387-35586-3_46)

1. INTRODUCTION - METHODOLOGY

In this paper, the term “e-vote” (electronic voting) is used to denote a voting process, which enables voters to cast a secure and secret ballot over the Internet or an Intranet (in the case of “internal” elections or decision making). In the framework of this paper, an e-voting process may fall in one of the following four categories:

- a) *Public elections and/or referenda* at state and/or local level (with binding effects).
- b) *Internal elections and similar decision procedures.*
- c) *Advisory polls* for decision-making and advisory referenda.
- d) *Internet polls.*

The aim of this paper is to discuss whether an e-voting scheme could meet the constitutional and other legal requirements, as these are laid down in the international legal and regulatory framework. The paper deals with how an e-vote process should be designed and implemented in order to comply with the democratic election principles and rights as well as to other human rights, which constitute the cornerstone of the international legal civilization. These issues are discussed in the light of the voting principles and rights of the users involved in an election process, which are similar within the European Union member states.

The scope of the paper is not limited to the general public elections, but also includes every election or decision-making process, which takes place through voting. It extends also to (Internet or Intranet) polls without binding effects (if the latter - in view of their nature or their extent - could influence the public discourse in a given state or organization).

The significance of the issues addressed herein is clearly manifested by the volume of debate that lately has begun on them, in many countries over the globe. This is understandable in view of the fact that technology usually moves at a pace faster than the legal system does. However, technological evolution should always be pursued as a means to improve human life as opposed to an end by itself. In this respect, all technological development, in particular those directly or indirectly affecting fundamental principles should be carefully reviewed with an eye towards determining their contribution to the betterment of society. Despite the volume of material published to support this debate, including user requirements specifications, no consolidated view on the requirements deriving from constitutional and legal consideration is available. This is the main contribution of the paper.

The paper is structured as follows: In section 2, the main issues associated with e-voting in public election processes are discussed. Section 3 addresses requirements for an electronic voting system to be used in general elections. Section 4 discusses requirements stemming from the democratic nature of the election process. Finally, section 5 summarizes our conclusions.

2. E-VOTING FOR PUBLIC ELECTIONS: MAIN ISSUES

The fundamental challenge of e-democracy is to improve and develop representative democracy towards processes based on the empowerment of citizens [7].

The new civilization brought about by ICT cannot and should not ignore the principles and values of democracy. The introduction of an e-voting system must also conform to this rule.

Voting is undoubtedly one of the functions “e-citizens” would like to see performed online. On the other hand, two items must be considered:

1. The *digital divide* and
2. The *inherent distrust* in an e-voting procedure.

An election system itself may enforce unequal access of an individual to the electoral process [18]. It is a matter of democracy, equality, and equity to guarantee that the different voting technologies are equivalent with respect to ease and opportunity of access. As long as the digital divide has not been overcome, e-voting should be viewed only as a supplement to – and not a replacement of – traditional paper-based voting. In this phase, e-voting cannot be considered as compulsory but, rather, as a supplemental alternative option for voters [6,12].

Any technology used in the context of an e-vote process must meet a set of baseline constitutional requirements. It is commonly accepted that parliamentary elections have to be free, equal and secret. At the same time, the election procedure has to be transparent and subject to public scrutiny. The constitutions of the European Union member states demand that the general elections must be General, Free, Equal, Secret, and Direct. Adding to these the fundamental requirement of Democracy, and analyzing these requirements to the next level of detail we obtain the first-level legal and regulatory e-voting requirements, which are summarized in Table 1. These will be discussed in detail in the sequel.

3. ELECTION PRINCIPLES

The **universal suffrage** is a basic principle for democratic elections. According to this constitutional requirement, every eligible voter can participate in the election process and nobody can be – directly or indirectly – excluded or discriminated.

Table 1: Overview of (first-level) legal and regulatory requirements for e-voting

S/n	Constitutional requirements	Generic (first-level) requirements list
1	General	1.1 Institutionally equivalent to traditional 1.2 Eligibility (registration and identification)
2	Free	2.1 Uncoercibility 2.2 No propaganda in the e-voting site 2.3 Non-valid voting capability
3	Equal	3.1 Equality of candidates 3.2 Equality of voters 3.3 One voter – one vote
4	Secret	4.1 Secrecy 4.2 Balance security vs. transparency
5	Direct	5.1 Not monitored ballot recording and counting
6	Democratic	6.1 Trust and transparency 6.2 Verifiability and accountability 6.3 Reliability and security 6.4 Simplicity

The consequences deriving from the principle of general elections are the following:

1. Every voter has the right to participate in an election process.
2. The ability to participate in an election process (eligibility) must be founded on the law and should be controllable according to the law.
3. Voting possibilities and technologies should be accessible by every voter.
4. Due to the lack of necessary infrastructure and to the digital divide, e-voting should be considered as an alternative way of exercising one's voting rights.
5. The democratic principle, i.e. every eligible voter should be included in the election process, results in the necessity for publicly available appropriate infrastructure (e.g. public internet kiosks, internet voting in government offices, etc.), in order to allow citizens to exercise their voting rights.

E-voting improves the generality of election procedures by providing an additional option of participation in the electoral process [18]. An essential question is whether the participation in the election through e-voting should be subject to the proof of special conditions as is the case with postal voting.

In most countries where postal voting has been established, only specific categories of individuals are allowed to exercise this option. Adopting an e-vote capability as an exceptional one (i.e. on the ground of the proof of a special condition, which prevents the eligible voter from physically casting his/her vote), is - from the legal point of view - a legally and constitutionally "safe" choice.

Against this opinion, founded on the historical and legal basis that voting in a physical voting station constitutes the rule, the following argument may be expressed: the evolution towards an information society has a significant impact on the ability of a citizen to exercise his/her rights and liberties. In the light of the political decision to improve e-government and e-participation, the introduction of an e-voting capability should be viewed as an institutionally equivalent and not as an exceptional option. In any case, such restrictions or other reservations do not seem to form an obstacle to the adoption of e-voting procedures.

Eligibility can, at the first stage, be ensured through the registration of voters, who meet the requirements of eligibility, and through the identification of the citizens at the moment of registration. (Secure) Registration and authentication are the means to ensure that the principle of universal suffrage is being respected and that elections cannot be rigged.

The purpose of voters' registers is to guarantee that only people eligible by law to vote can do so, and that no one can vote more than once. A question arising at this point is whether there is a need for a specific registration process in the case of e-voting. E-voting is, in many ways, analogous to postal (absentee) voting. Where such a voting capability is introduced, a proper authorization or registration process is usually required. Such a procedure does not affect the principle of general elections for the following reasons:

- Supposing that there is no country wide, online voter register, a pre-registration for e-voting is necessary in order to avoid vote fraud. Such a registration supports the integrity of elections. For the same reason, an Internet-based voter registration system is not recommended because it could be vulnerable to large scale and automated vote fraud. [11]
- E-voting is considered as an alternative capability, which may facilitate the participation of the voters. Taking into account the associated organizational difficulties, a specific registration or declaration that the voter is willing to make use of the e-voting option constitutes neither exclusion nor discrimination.

Providing a secure identification and authentication scheme of eligible voters is a *conditio sine qua non* requirement for any public-election oriented e-voting system.

Moreover, since the requirements concerning integrity must also be taken into account, it must be ensured that it is easy for voters to register and authenticate themselves for e-voting. Otherwise, too complicated registration and authentication methods could be a burden to voters [4].

The principle of **free elections** requires that the whole election process take place without any violence, coercion, pressure, manipulative interference or other influences, exercised either by the state or by one or more individuals. Regarding the postal voting case, the Dutch legislation requires that the voter has to sign a declaration on the vote-by-mail certificate that he/she has filled out the ballot personally. Providing such a signature does not seem so easy in the case of e-voting, although similar options should be provided [5].

However, e-voting procedures may indeed pose new threats to the freedom and integrity of voters' decision, beyond those that postal voting does. This becomes obvious in the workplace: even if the employer, the supervisor, or a colleague are not standing over the shoulder of the employee-voter intranets, system administrators may monitor or record the activity at each workstation and obtain a copy of the ballot [13]. Moreover, the distributed nature of the Internet could facilitate large-scale vote selling or trading.

Uncoercibility and **prevention of vote buying** and extortion can be ensured by an e-voting system designed so that no voter can prove that he/she voted in a particular way (untraceability on the part of the voter) [1]. Since the employment relationship is not balanced, it is suggested to avoid e-voting from the workplace. In any case, coercion can hardly be prevented by technology alone. A possible solution is to develop a public accessible infrastructure, in public and controlled physical sites, thus allowing voters to exercise their rights free of the coercion of any third party.

The **freedom of decision** may be violated if a propaganda message is blended on the computer screen, while the voter is casting her/his electronic ballot. In the existing election schemes it is not allowed to advertise in (the vicinity of) the polling place. Thus, the e-voting procedure should make technically infeasible the advertisement of political parties/candidates on the e-voting website.

The democratic legitimatization of e-voting relies on satisfying the generic voting criteria of a democratic election system. This includes the **free expression of the preferences** of the voter, even through casting a non-valid or a "white" paper ballot [16]. In order to preserve the freedom of voters' decision, the possibility for casting a consciously invalid vote should be provided and guaranteed.

The requirement of **equality** in the context of public elections is a specific expression of the principle of equality. It constitutes one of the

cornerstones of modern democracies. Under the principle of equal suffrage, two major requirements are identified:

1. Equality regarding the political parties, candidates etc., who participate in the public elections.
2. Equality regarding the voting rights of each voter.

A requirement deriving from the principle of equality is that electronic ballots should be edited and displayed in a way analogous to that used for the paper ballots. Electoral equality requires that there are no deviations between the printed ballot and its electronic equivalent. Furthermore, the placement of electronic ballots in the (public) voting site (i.e. on the screen of the e-voting site) should ensure equal accessibility. Thus, the structure and appearance of site and ballots should not favor or discriminate against any of the participating parties.

Another element of equality among the parties to be elected is that the decision of the voter, as expressed through the online ballot, is transmitted and counted without changes or/and interferences. A valid cast vote must not be altered or removed in the course of the voting process.

Transparency should also be supported. All parties should have the opportunity for equal access to the elements of the voting procedure, in order to be able to establish its proper functioning.

The principle of equality requires that each vote, physical or online, is equally weighted towards the election outcome. In an e-voting situation, certain voters have an access advantage to the enabling technology and, therefore, to e-voting capability. Some argue that remote Internet voting could be used to manipulate election outcomes by structuring access to favor those who are the most Internet – connected [15].

In view of the current technological and societal trends, the right to “equal accessibility to the voting process” must be extended to the right of “equal accessibility to election technology”. An adequate, non-discriminating procedure should be offered to the voters, in order to allow them to efficiently exercise their voting rights with no obstructions. As a result, universal access may become a constitutionally indispensable requirement [2]. Equal accessibility means also that the system should be user-friendly, and independent of the voter’s education, age and physical condition (to accommodate physically disabled voters).

An e-voting system should ensure that the “**one voter, one vote**” principle is respected. In other words, the system should ensure that only eligible voters vote. Every voter can vote only once for the specific election, either online or off-line. Therefore, an e-voting system should be designed in such a way as to prevent the:

1. “duplicability” of the vote (either by the voter her/himself or by someone else);

2. “reusability” of the vote (either by voting more than once online or by voting both online and offline);
3. “modification” of the cast vote (after a voter has dispatched her/his vote).

A related issue is the **duration of the voting period** for e-voting. The California Internet Voting Task Force suggests that Internet Voting does not continue throughout the election day, i.e. that there should be a time in advance of the election day, fixed by law, when e-voting is cut off. In order to facilitate access to e-voting, it is further suggested that the voting period be extended for more than one day. This possibility may result in two issues:

1. In most European Union member states the elections take place on one day only. In these cases the constitutional and legal provisions should be amended.
2. The principle of equality is put in question, especially if e-voters could make use of this possibility for more than one day.

Secrecy and freedom are strictly related principles: Secrecy is the precondition of the voter’s free political decision. In democratic elections the link between the vote and the voter must be irreversible, in order to ensure that votes are cast freely. In traditional voting procedures the secrecy is “physically” protected, but e-voting may make virtual voting vulnerable to violations of secrecy.

The following requirements are derived from the principle of secrecy:

1. The secrecy of the vote has to be guaranteed during the casting, transfer, reception, collection and tabulation of votes.
2. None of the actors involved in the voting process (organizers, election officials, trusted third parties, voters etc) should be able to link a vote to an identifiable voter.
3. There must be a clear and evident separation of registration and authentication procedures and casting-transfer of the vote.
4. No voter should be able to prove that he/she voted in a particular way. Confirmation of the vote, after the ballot has been transferred and received, enforces the confidence in the system and ensures the rights of the voter but it cannot relate to the content of the vote.

The electoral provisions that are applicable to postal voting, as well as to the protection of communication secrecy, could also serve as a basis for solving the problem of “**political privacy**”. However, there can be no guarantee of the freedom from external influence by third parties during the casting of votes. This constitutes an inherent risk of any form of remote voting. To face this risk, measures should be taken on the policy and regulatory levels, in order to impose compelling and enforceable measures against coercion and to sanction illicit behavior.

Secrecy has to be in harmony with the other democratic principles for public elections. Ballot secrecy should be reconciled with transparency and auditability of the entire voting process. The election system must be able to allow the verification of the authenticity of the ballot before the votes are viewed or counted. In order to protect secrecy, the voted ballots should be decrypted and counted after the authentication information is reviewed and “removed”. The e-voting system should be designed in such a way as to make vote control and recount technically feasible, without re-identifying the voters [10,17].

The principle of **direct election** states that there can be no intermediaries in the process of voting decision. This principle may be well adapted to fit an e-voting procedure. The relevant requirement is that each and every online ballot is directly recorded and counted. A problem may arise in the case where the voting period differs with the voting procedure (online or off-line) used to cast the vote. Online voting results may influence the outcome of the entire election process and limit the integrity and legitimacy of the whole process. A suggestion is to develop a system that allows the recording and maintaining of the cast vote, while prohibiting any counting before the end of the (off-line) voting period.

4. PRINCIPLES OF DEMOCRATIC VOTING

A democratically designed e-voting procedure should, at least, meet the requirements of a traditional election system. However, additional requirements must be also met, particularly due to the remote nature of e-voting. These requirements pertain to the preservation of attributes and properties, such as the transparency, accountability, security, accuracy, legitimacy and to the democratic legitimization of the election system.

Voters should be able to understand how the elections are conducted. The traditional voting “technology” operates in a way that is transparent to the voters and to the other election actors, since in most countries votes are counted in the presence of the parties’ representatives. On the contrary, online voting procedures are not transparent, because the average voter does not have the knowledge necessary to understand how the system works. As a result, in the case of e-voting, much more trust in the technology used and the persons involved (election officials, technology providers etc) will be required by the voters.

Verifiability is strongly related to transparency. The e-voting procedure has to be able to allow verification by voters (individual verifiability) or by election officials, parties, independent observers (institutional verifiability), etc. However, verifiability is orthogonal to secrecy (confidentiality), in the

sense that individual verifiability (i.e. the possibility of a voter to verify his vote and receive confirmation about casting and counting of its vote) is clearly conflicting to the requirement of secrecy, as a condition of free choice.

An additional requirement is the **accountability** of the system, meant as the logging and monitoring of all operations related to e-voting.

The **reliability** and **security** requirements are derived by the democratic need to ensure that the outcome of the election reflects correctly the voters' will. A reliable system should ensure that the outcome of the voting process corresponds to the votes cast, i.e. that it guarantees eligibility, secrecy, equality and integrity. The ballot that is transmitted to the voting counting equipment must be an accurate and not modifiable copy of the voter's real choice (integrity). Moreover, it should be infeasible both to exclude a valid vote from the tabulation, and to validate a non-valid one.

Security is a multidimensional notion in the context of e-voting. Security primarily refers to the (technically guaranteed) respect of secrecy and freedom but it covers the entire range of functions and election components such as registration, eligibility and authentication. In addition, security refers also to the availability of the system. The system must be protected against accidental or intentional denials of service and must be available for use whenever it is expected to be operational. Unavailability of the system (or of one of its components) may result to loss of the capability of a voter to exercise his/her fundamental political rights.

Traditional voting systems are relatively simple. On the contrary, e-voting systems are inevitably complicated; furthermore, they usually involve more actors than traditional systems do. From the point of view of the voters, the system should be easy to use and should require no particular skills. As a result, an e-voting system should be developed in such a way as to facilitate its usability and to preserve its controllability.

Simplicity and **accessibility** of a system are not merely technical issues. They require additional educational, as well as organizational measures (help desks, e-election officials, etc.), to be effectively resolved.

Based on the above principles, the following second-level (functionality-oriented), requirements are derived:

1. There must be trusted certification procedures for hardware and software.
2. The entire infrastructure (including source code), as well as every system's functionality, must be logged.
3. All operations (authentication, vote recording, vote tabulation etc) should be monitored, while secrecy is preserved.
4. The infrastructure should be open to inspection by authorized bodies.

5. Voters, parties and candidates must be ensured that there has been no malpractice.
6. Adequate system security must be ensured.
7. The system must be simple and user-friendly.

5. CONCLUSIONS

Knowing that information and communication technologies are only instruments, politicians and legislators have a clear duty to meet the citizens' democratic demand to promote day-to-day democracy and to encourage citizens' participation. Technology should serve the goal to face the crisis of confidence that representative democracy is experiencing today.

The right to vote is only one part of the democratic process, but it remains a civil right deeply embedded in Constitutions and is considered to be one of the primary foundations of democracy. Hence, e-voting is not like a common electronic transaction. An e-voting procedure will only be acceptable under the condition that it safeguards the constitutional principles associated with the voting process, such as equality, freedom, secrecy, transparency and accountability.

Furthermore, such a procedure should be enacted in a general framework promoting equal access to ICT infrastructure. This must be open, accessible, interactive and secure, in order to enable citizens to participate in political life and have a direct impact on it.

For the foreseeable future, e-voting systems can only be pilot projects. Assuming that the relevant legal and the resulting "technical" requirements are met, e-voting systems will become a possibility for all citizens. Otherwise they will not promote democracy; they will simply serve to reconstruct new political elites.

References

1. Adler J., Internet Voting Primer, www.votehere.net/adacompliant/whitepapers/primer.
2. Burkert H., "*Elektronische Demokratie: Einige staats und verfassungsrechtliche Anmerkungen*", <http://www.gmd.de/People/Herbert.Burkert/> ARCHIV.
3. Buttler R., et al., "A national-scale authentication infrastructure", *Computer* Vol. 33, no. 2, pp. 60-65, February 2000.
4. California Institute of Technology – MIT, Voting Technology Project, *Voting: What is, What could be*, July 2001.

5. Cybervote Project, *Report on electronic democracy projects, legal issues of Internet voting and users requirements analysis*, European Commission, IST Programme, 2000.
6. Dix A., "Electronic democracy and its implication for political privacy", in *Proc. of the 23rd International Conference of Data Protection Commissioners*, September 2001, Paris.
7. European Commission, IST 2000 Programme, *The Information Society for all*, Final Report, Brussels 2000.
8. Hoffman L., Cranor L., "Internet voting for public officials", in *Com. of the ACM*, Vol. 44, no. 1, pp. 69-71, January 2001.
9. Holmes N. "US electorate reform: The obvious obligation", *Computer*, Vol. 34, no. 2, pp. 126-128, February 2001.
10. International Working Group for Data Protection in Telecommunications, *Common Position on the Use of the Internet in the Conduct of Elections*, Berlin, September 2001.
11. Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, March 2001.
12. Jones B., *A report on the feasibility of Internet voting*, Internet Voting Task Force, State of California, January 2000.
13. Kim A., "Ten things I want people to know about voting technology", Democracy Online Project's National Task Force, California Voter Foundation, January 2001.
14. Mercuri R., "Voting automation (early and often)?", in *Com. of the ACM*, Vol. 43, no. 2, pp. 176, February 2000.
15. Phillips D., von Spakovsky H., "Gauging the risks of Internet elections", in *Com. of the ACM*, Vol. 44, no. 1, pp. 73-85, January 2001.
16. Rieß O., *Wahlen im Internet, quelle multimedia und recht*, <http://www.Internetwahlen.de/project/ruess.html>.
17. Schoenmakers B., *Compensating for a lack of transparency*, <http://citeseer.nj.nec.com/schoenmakers00compensating.html>.
18. Tauss J., Kollbeck J., e-vote: Die elektronische Briefwahl als ein Beitrag zur Verbesserung der Partizipationsmöglichkeiten, www.tauss.de/bn/e-vote.html.