“CONSTITUTIONAL AND LEGAL REQUIREMENTS FOR E-VOTING”

1. Introduction

Voting is one of the primary foundations of democracy. Existing voting legislation and non-electronic voting systems have been developed over the years in a way that ensures that the principles required for democratic elections and referendums are met. The significance of these issues is clearly manifested by the volume of debate, which lately has begun on them as well as by the increased number of projects and pilot e-voting procedures, in many countries over the globe. There are a number of technological products and programs already available on the market. 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 improvement of society. Any attempt to introduce e-voting will have to address a series of complex constitutional and legal issues.

This paper1 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

---

1 This paper is based on a research in the framework of the project E-vote. The e-VOTE system is an internet-based electronic voting system that provides all the required services for organizing and conducting a voting process, supporting both election organisers and voters. The development of the system has been supported in part by the European Commission [ IST Programme, Project e-vote (An Internet-based electronic voting system; IST-2000-29518)]. The consortium consists of partners from five European countries, namely: Q&R International S.A., University of the Aegean, University of Regensburg, Cryptomathic SA, Municipality of Amaroussion (Greece) and Kosice Self-governing Region (Slovakia). The project's start date was 1st October 2001 with a duration of 30 months. The results of the project have been documented in the project deliverables that can be accessed at www.instore.gr/evote.
constitutional rights, which constitute the cornerstone of the European legal civilization, like the right to personal data protection. In this paper, the term e-voting (electronic voting) is used to denote a remote voting process. It focuses on the analysis of the election principles to be met in the frame of e-voting. It addresses requirements for an electronic voting system to be used in general elections. As far as it concerns public and binding election procedures, an electronic voting process must respond to constitutional requirements, primarily derived from European constitutional texts. An e-vote process has to be designed in such a way as to guarantee the general, free, equal, secret and in principle direct character of elections. In a democratic context, an electronic voting system must respect and ensure attributes and properties such as transparency, verifiability, accountability, security and accuracy. Only then can it foster and promote the participation of citizens, as well as the legitimacy and the democratic transaction of the election process.

My assertion is, that these requirements (should) cover every election or decision-making process, that takes place through voting, if they could influence public discourses and processes [31, 32]. In light of their high significance, the emphasis of this contribution is put on public elections. Discussed are further requirements stemming from the democratic nature of the election process. Emphasis is given on the recently presented/published “Draft Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting (approved by the Multidisciplinary Ad Hoc Group of Specialists on 5-6 July 2004). The constitutional and legal problems raised in the context of e-voting also are dealt in the light of the Universal declaration on Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, the so called Copenhagen Document of 1990 of the Organisation for Security and Co-operation in Europe.

2. What is e-voting? From a technical to an institutional definition

Under the term e-voting (electronic voting) we usually understand 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)[7, 25], while some reports/ authors distinguish the terms e-voting and remote e-voting. A key element is the remote vote casting nature of the procedure. Another important element is the need for computing equipment, as well as for communication means for a citizen to exercise his/her voting right.

In the Council of Europe’s draft Declaration e-voting is defined as “an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote”. As remote e-voting is understood an e-voting procedure “where the casting of the vote is done by a device not controlled by an election official”; I would propose that we should adopt the definition of the Council of Europe’s Recommendation, which is not based solely on means used but rather on the main problem that we have to face, the fact that e-voting is becoming a “private” and un-controlled act. The distinction between supervised and unsupervised electronic voting highlights the level of control that those responsible for elections can exercise over the voting process.
Supervision serves the need to ensure that the voter has the opportunity to cast the ballot in secrecy and without coercion, that the vote is not intercepted or altered and that personation or multiple voting is prevented. [7,25,30] This lack of control concerns not only e-voting procedures. Once remote voting is widespread the voting process will be as a whole largely unsupervised, at least in traditional terms.

3. Standards for e-voting: ...as fair, free, secret, secure and reliable as the traditional elections?

The increasing use of new technologies enables and sometimes obliges and forces governments, administrations and citizens to establish new forms of relationships between them. The Information and Communication Technologies (ICT) revolution has already generated huge changes in economy and society that bear major implications for democracy and governance: The evolution of the information society has a deep impact on all aspects of people lives, including their ability to exercise their democratic rights and civil responsibilities. The fundamental challenge of e-democracy is to improve and to develop representative democracy towards processes based on and aimed at the empowerment of citizens. The need to maintain a central position in social processes and to adapt to the rapidly changing structures of communication in the information society, has led governments and international organizations (to try) to offer new ways and possibilities of participation and services through networks. [32]

Over the last years there has been strong interest in online voting as a way to make voting more convenient and attractive, with the intention of coping with (to some extent) the problem of increasing abstention rates (especially among younger people, foreign residents, business and holiday travelers, handicapped and elderly). [7, 25] However, rather than focusing upon increasing turnouts or enhancing voter convenience, the issue is compound one of creating a flexible and robust system, in order to make voting a tool for public discourse and policy making.

Any implementation of e-voting, therefore, must fit the criteria of maintaining or enhancing the robustness of electoral processes while, at the same time, demonstrating real benefits to citizens. The introduction of new voting procedures must depend on their capacity to provide at least the same level of "guarantees", which are designed and provided for traditional voting procedures. It is commonly accepted that parliamentary elections have to be free, equal and secret [7,15,16,19,23,26]. Furthermore, the principles of universal and direct suffrage belong to the European electoral heritage. The principles of freedom and secrecy, as well as the reference to fair elections are enshrined, explicitly or implicitly in a number of international instruments like the Additional Protocol to the European Convention on Human Rights or the International Covenant on Civil and Political Rights [54]. At the same time, the election procedure has to be transparent and subject to public control and scrutiny. Moreover, a democratic e-voting system should ensure integrity, availability, reliability, security and accountability.

It is essential that these principles are not undermined by the introduction of new voting methods. “Only those e-voting systems which are secure, reliable, efficient,
technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting” [13]. Accordingly, e-voting systems must be so designed and operated as to ensure that they should be as fair, free, secret, reliable and secure as democratic elections and referendums, which do not involve the use of electronic means. Furthermore the introduction of an e-voting system conforms to the abovementioned demands if it is designed to encourage citizens’ participation, in a quantitative (more voters) and a qualitative (more informed voters) way.[32]

The Council of Europe’s Draft Recommendation introduces three categories of standards, which include provisions relating to all stages of elections and referendums (pre-voting state, actual casting of vote and post-voting stage). The legal standards, reflecting the fundamental principles of elections enshrined in international legal instruments, relate to the legal context in which e-voting is permitted. The operational standards, pertaining to basic matters of organisation and procedure with regard to e-elections, relate to manner in which hardware and software should be operated and maintained. Finally, the (core) technical requirements, relating to the construction and operation of hardware and software, should ensure the technical security, accessibility and inter-operability of e-voting systems [13/39]

Special emphasis/importance is given by the Council of Europe on the close interconnection between the three categories of standards [14], which can relate to one, two or all stages and has to be taken into account when applying the Recommendation. I would prefer to describe this interconnection as a “complex electoral interdependence model”, which manifests the interdependence of law and technology, where the latter (the technology) offers new possibilities and, consequently raises new problems, that the first (the law) has to resolve. Actually, the legal, operational and technical requirements depend on each other and they cannot be isolated. Legal standards are (more than) necessary to establish the public policy objectives, but insufficient to ensure the implementation of constitutional principles and fair electoral practices: operational and technical standards should ensure respect of the legal standards. On the other side, in effect legal regulation shares rule making and guaranteeing authority with technological standards and protocols. In this context, attention must be paid to the risk that available market products, developed as a response to a technical problem in a law-myopic fashion, could influence the choice of policy and the implementation of the law.

A crucial difficult refers to the need to harmonise the various requirements to each other. 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. Universal suffrage (and accessibility) principle requires simple means and methods, which perhaps constitute an additional obstacle to a robust and secure voting system. [32]
4. Fundamental Principles

4.1. Universal suffrage

According to the constitutional requirement of universal suffrage, every eligible voter can participate in the election process and nobody can be - directly or indirectly - excluded or discriminated. The principle of universal suffrage primarily requires that every voter has the right to participate in an election process, while voting possibilities and technologies should be accessible by every voter.

4.1.1. Access as a democratic prerequisite and condition for confidence

A key parameter of e-voting procedures pertains to the need for computing equipment, communication means and the respective knowledge for a citizen to exercise his/her voting right. Differential access to technology and technology use proves to be a primary concern in relation to the acceptance and the assessment of e-voting, as far as it concern two core principles of democratically conducted voting, i.e. universality and equality.

Differential access to online technology would be a serious issue and is a primary concern. The digital divide, i.e. the lack of equal access opportunity to the Internet and to the ICT infrastructure means is extremely important, especially in the case of public elections. The problem becomes more complicated, taking into account that secure online voting would require not just Internet access, but also additional security means to be available to the voter, such as, for example, a digital certificate [28]. Offering new forms and possibilities of participation, based on Information and Communication Technologies (ICT), could lead to the exclusion of “ICT illiterate” voters from the e-electoral body. The experience gained in several countries leads to the conclusion that any election system can result in unequal access to the electoral process. There are certain (categories/groups of) voters, who by having an access advantage to technology, will be (unfairly?) advantaged by the implementation of remote online voting capabilities. Given that studies of internet users consistently show that they are younger, more affluent and more educated than no users, switching to e-voting runs the risk of actually widening the existing participation gap between the more and less advantaged sectors of society. [22,32]. According to the Council of Europe’s approach, from the principle of universal suffrage derives the requirement that “the voter interfaces of an e-voting system shall be understandable and easily usable by as many people as possible” (CoE, Standard No 1).

The kind, as well as the accessibility of the voting procedure affects the principles of universal and equal suffrage, which are among the cornerstones of democratic elections. The digital divide can lead to inequalities and (indirect) discrimination. The introduction of e-voting could widen the access (as well as the participation) gap, as there is no prior guarantee that no population group will be excluded from the democratic decision making process [5,33]. From this perspective the digital divide and access disparity constitute a critical shortcoming for the feasibility and
constitutionality of e-voting procedures. Therefore, in view of the access disparity and of the relevant risks, an e-voting procedure could be introduced only as an additional and optional means of voting. [17]. This is also the opinion followed by the Council of Europe, which stresses the point that “adding additional electronic voting channels to traditional forms of voting may make elections and referendums more accessible, strengthening the principle of universality. However, using a single remote electronic voting channel in isolation restricts accessibility”. Council of Europe refers explicitly to its purposes: This provision is to protect the voter from a situation where the only means offered for voting is one that is not effectively available to him or her.”[14]

One of the dangers is that e-voting could easily be used to manipulate election outcomes by structuring access to favour those who are the most Internet-connected [36,46], thus granting the more advantaged groups of society potentially greater influence over the election outcome. Undoubtedly, the possibility of a citizen to vote at home is a “privilege”, which could be counter-balanced by the legitimate purpose, i.e. by increasing citizen participation and, consequently, the enlargement of the base of democracy. However, differential access is an essential problem, not only in terms of equality of the voters. It also impinges upon the principle of fair elections and to the functioning of democracy; accessibility and usability of voting technology could be regarded as a critical factor, influencing the outcome of elections[32]. Differential technological penetration might compromise the fairness of the electoral process [55].

Electronic voting will become democratically acceptable only when the majority of the eligible voters have easy access to the Internet [35]. An adequate non-discriminating procedure should be offered to the voters, in order to enable them to efficiently exercise their voting rights without any obstructions. From this perspective, the notion of universal access is not only critically important for ensuring social acceptability of ICT technologies and of the emerging Information Society [49]; it eventually becomes a constitutionally indispensable requirement [6]. In view of the current technological and societal trends, the right to “access to vote” must be extended to an interest in equal access to voting infrastructure [46]. Overcoming the digital divide by general access of the electorate to Internet polling stations or at public access points (kiosks) could be proposed as a solution, although “walking to the e-center to cast an electronic ballot hardly seems like much of a technological leap”.

4.1.2. E-voting as an exceptional option?

As e-voting improves the generality of election procedures by providing an additional option for exercising political rights [50], it prima facie raises no specific problems in relation to the principle of universal suffrage. A preliminary and essential question is whether the participation in an election through e-voting should be subject to the proof of special reasons.

Do we have to distinguish e-voting, as a form of absentee voting, based on need and absentee voting based on demand? Offering the option of remote voting for voters who are obstructed for some specific reason is undoubtedly in conformity with the principles of equality and universal suffrage, since it is justified by a difference of situation. Some argue that there is no constitutional requirement to provide absentee voting and especially e-voting on demand [24]. Adopting an e-voting 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, well founded on the historical and legal basis that voting in a physical voting station is and should remain the rule. An additional argument concerns the fact that in most countries where postal voting, as a form of absentee/remote voting, has been established, only specific categories of individuals (usually voters who reside abroad) are allowed to exercise this option. In some countries postal voting is allowed only if the voter applies for this option on important grounds (infirmity, illness, absence, etc.), which prevent him/her from voting in his/her electoral district during voting day/hours.[32]

On the other hand e-voting, like postal voting, improves and broadens the principle of universal suffrage [44]. But the decisive argument is that the exceptional (and supplementary) nature of e-voting would indicate (and at the same time result to) a loss or reduction of interest for innovation and for technologically supported participation in political processes. 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. [31].

4.2. Equality

The principle of equality further requires that all participants, be they candidates or voters, should have equal chances and (voting) rights. Equality of suffrage can also be endangered if the use of new technologies makes voting unavailable to some voters. From a purely legal point of view, making e-voting possible is not contrary to equal suffrage as long as non-initiated voters are given a similar possibility to express their choice. E-voting, like vote by mail, could be offered only to voters, who are not able to go to the polling station. This would not be contrary to the principle of equal suffrage since it would be justified by a difference of situations, but, as already mentioned above, it would strongly reduce the interest of the innovation [21]. However, as one of the main reasons for introducing e-voting is increased accessibility and opportunity for voting, and because in all known cases and recommendations, e-voting is only an additional option, equality of suffrage is unlikely to be violated in practice.

The principle of equality results not only in the right to equal accessibility to the election technology. It is furthermore required that each vote will be weighted equally towards the election outcome. Every vote deposited in an electronic ballot box should be counted, and each vote cast in the election or referendum should be counted only once. The Council of Europe adds to the legal standards pertaining to equal suffrage the requirement that if electronic and non-electronic voting channels are used, there should be a secure and reliable method to aggregate all votes and to calculate the correct result.[32]

E-voting could carry a risk of violating the principle of equal suffrage if it allows for multiple voting, family voting, forced voting, voting by non-voters or vote trading. This risk is not new, since it is also present with postal voting, when it is anonymous. An e-voting system must therefore ensure that the “one voter, one vote principle” is respected. In other words, such a system should prevent: duplicability and reusability of the vote: A voter should be prevented from voting more than once online or by more than one voting channel [19]. It is particularly important, where remote e-voting
takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once (CoE – Standard No 44).

Further, the systems should not allow the “modification” of the cast vote (after a voter has dispatched her/his vote). In some member states practices are in force where it may appear that a voter is allowed to vote more than once. In the case of Denmark and Sweden, the voting systems provide the legal opportunity for voters to submit an advance vote and change it later. In Denmark, several advance votes may be submitted. In Sweden, only one advance vote may be submitted. In both systems only the last vote is inserted into the ballot box and thus is the vote cast. However, in these systems the voter may cast only one vote, which is finally counted. [14]. The legal opportunity to submit a vote (on-line) and to change it later (off-line) is proposed by some authors in order to face the problem of voting online under pressure either in the family or the workplace environment. However, this legal opportunity could hardly be accepted, as it would be regarded as a violation of the principle of equality.

A critical issue, strictly related to equality, concerns the definition and duration of the voting period. Preventing multiple voting may require the definition of different voting periods for the various voting modes. The definition of a longer voting period may put in question the principle of equality [36] and raise constitutional issues, where it is provided that general elections shall be held simultaneously throughout the State. Where voting by mail has already been introduced, this problem has been solved by counting the mailed in ballots simultaneously with the physically cast ballots [15]. The possibility to cast an online vote should be temporally limited to the period in which postal voting is allowed [2]. On the other side, technical constraints and potential risks dissuade from limiting e-voting to one day only and especially to the election day, taking further into account that a possible unavailability of the system may deprive the voters of the capability to exercise their voting rights, which could result on its turn to another violation of equality. [7] The Council of Europe in its draft Recommendation accepts that remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.

It is further suggested to extend the voting period to more than one day, so as to facilitate and encourage access to e-voting. However, such changes as the proposed extension of the Internet polling periods even to three weeks, could and probably would have profound effects on both voting behaviour and political campaign techniques, with possibly further consequences to the integrity of elections. [23]

4.2.2. Simplicity as a matter of accessibility and e-equality

Another dimension of accessibility concerns the voter capacity to use the technology to vote. Traditional voting systems are relatively simple. On the contrary, e-voting systems are inevitably complicated; furthermore, they usually involve more acts and actors than traditional systems do. Additional complexity appears sometimes to be the inevitable price of increased security and integrity of the system [32]. However, willingness to make use of and benefit from new voting possibilities is intrinsically
linked with the experience of using the technology interactively [30]. The recent case of the State of Florida indicates that even low complexity in technology may result in very serious consequences for the legitimacy of the elections. Equal accessibility, as a precondition of democratic participation, means that the e-voting system to be introduced should not be complicated, i.e. it must not be “a test of computer literacy” [8]. From the voters’ point of view, the system should be easy to use and should require no particular skills. On the contrary, it should be user-friendly and independent of the voter’s education, age, and physical condition [19]. 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.

4.2.3. Universal access and equality for voters with disabilities

As mentioned above, a requirement deriving from the principles of universal and equal suffrage concerns the usability of the e-voting system independently of the voter’s physical condition. People with disabilities are still excluded from full participation in society, including active participation in political life and the right to vote as they are often faced with architectural, organisational and technical barriers (physically inaccessible polling stations, illegible ballots, inaccessible written information etc.). In many cases those problems lead to the situation that people with disabilities cannot cast their vote or cannot vote independently and in secrecy. Some countries have a provision that voters need to be able to read, write and count correctly in one of the official languages. This obviously requires people to be able to speak and excludes users of sign language. In some legal texts there is also a provision for “sanity” as a condition for the exercise of voter’s rights.

From a perspective of democracy and equality, it is vital that all citizens have access to and can use the electronic tools and channels used by governments and public authorities. Both accessibility and usability are key concepts when including persons with disabilities in the digital democracy. Achieving universal accessibility is part way towards the goal of achieving universal usability. The Council of Europe recommends that e-voting systems should be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.

4.3 Registration and identification as elements of equality and democracy

The voting right extends further to a right to exact composition of the electorate [2] (Secure) Registration and authentication of voters are the means of ensuring that the principles of universal and equal suffrage, summarized as “one voter, one vote”, are respected and that elections cannot be rigged [54]. Authentication is proved to be an
issue of freedom too, as the most serious violation of the freedom of voters would be the voter’s identity theft. [21] Voter registration systems and accurate voter registration lists are important for the integrity and the legitimacy of the election process. Any major compromise of the voter registration system could lead to election fraud. Providing a secure identification and authentication scheme of e-voters is a conditio sine qua non for e-voting systems to be used in public elections. [32]

Identification and authentication of the voter are important at the time of the registration and/or request for e-voting, in order to avoid fraudulent possibilities (“first phase” authentication). Authentication at the time of casting a vote is another important procedure, which ensures that only eligible voters vote (“second phase” authentication). Authentication is primarily ensured through the registration of voters, who meet the requirements of the law, and through the identification of citizens at the moment of registration. In the context of a traditional election procedure, voters are identified and authenticated in the polling station by the use of adequate identification tokens. First level (phase) identification and authentication, which can take place at the moment of registration, is more reliable than online authentication; it could thus be considered as an additional guarantee for second level (phase) authentication. Registration and authentication procedures should be accurate, complete, immune from fraud, dynamic and up-to-date. [32]

The Council of Europe regards as conceivable that online registration will be offered to voters (CoE, Standard No 40). Considered could be also that voters are enabled to apply for remote e-voting in an online or electronic way, for example after they have registered themselves. It should be noted that, for both possibilities, a very substantial effort will be necessary in order to solve the problems of identification and authentication in a remote electronic way. This implies the existence of some means of electronic authentication through, for example, a digital signature and the existence of electronic registers. A further question is whether there is a need for a specific registration process in the case of e-voting. Does such a procedure affects the principle of universal and equal suffrage or a pre-registration for e-voting will be considered as necessary in order to avoid vote fraud? Thus, such a registration supports the integrity of elections and it cannot be considered as exclusion or discrimination. However possible registration requirements should not pose an impediment to the voter participating in e-voting (CoE, Standard No 2).

4. 4. Free and secret suffrage

4.4.1. Free formation and expression of political choices

The principle of free elections requires that the whole election process take place without any violence, coercion, pressure, manipulative interference or other influences, that may be exercised by the state, an organization, or by one or more individuals. The voter must be able to vote personally and without any extraneous influence. Freedom of voters includes two main aspects: the freedom of voters to form their opinion and the free expression of this opinion. [32] This approach has been followed by the Council of Europe, when it recommends that “the organisation of e-voting shall secure the free formation and expression of the voter’s opinion and, where required, the personal exercise of the right to vote” (CoE, Standard No 9). Even if the Council
of Europe insists on personal suffrage, it considers, in order to ensure accessibility and universality, proxy voting as allowed, and possible within the e-voting standards.

The Council of Europe is conscious of the risks of “mouse – click – voting”. “The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection” (CoE, Standard No 10). The Recommendation strengthens the free formation and expression by requiring that voters should be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person (CoE, Standard No 11).

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 “blank” vote [40]. The Council of Europe shares this opinion, when requiring that the e-voting system should provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, e.g. to cast a blank vote (CoE, Standard No13). A further question concerns the invalid votes. In the context of traditional voting systems, such votes are either cases of error or consciously cast. The invalidation of the vote signifies a “sanction”, as the vote cannot contribute to the outcome of the election. On the other side we cannot deny that the deliberate invalidation of a vote entails a valuable (even not valid) democratic behaviour of the voter [4]. Therefore, the possibility for casting a consciously invalid vote must remain technically possible. However it is advisable that the voters be warned before casting a blank ballot, in order to avoid mistakes, due to a possible lack of technical capacity and experience [51], without ignoring that this warning could be interpreted as a manipulative interference in the voter’s decision.

By providing voters with an additional channel the introduction of e-voting has the potential to improve the quality of the choice. In order to promote the model of “informed and active citizen” Some authors argue for the provision of clearly designed menus, which allow the voters, before casting their votes, to visit sites of political parties and interest groups and rapidly locate the specific information they are looking for [2]. Without denying the significance of information and deliberation for the ability to exercise political rights, it should be emphasized that the interactive and informative use/usability of the e-voting site could result in an undue influence of voters. [32]

The Council of Europe recommends that the e-voting system should be designed and operated in a way that ensures that all kinds of manipulative influence are excluded (CoE, Standard No12). Through the design of the portal or the site information and choice could be guided into a specific direction. Moreover the temporal proximity of information and vote casting could result in emotional choices [4/5]. The requirements concerning free elections are applied in relation to the “online environment” of the voter. The freedom of decision may also be violated if a campaign message is blended on the computer screen, while the voter is casting her/his electronic ballot. In 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 [5,15, 52].

Coercion, vote buying and extortion are of great concern in connection with other methods of remote or absentee voting [17]. Where remote voting methods have been
constitutionally accepted, regulators and judges have attributed major importance to the attestation that the voter has filled out the ballot personally. Providing an attestation declaration through a digital signature, instead of a handwritten declaration, could serve as an institutionally equivalent and feasible solution.

4.4.2 Secrecy as element of freedom

E-voting procedures may indeed pose new risks to the freedom and integrity of voter decision. [30,35]. Free choice is strongly related to the question of secrecy in e-voting. Secrecy is the precondition of a free political decision, a defining principle of modern democracy [41] and remains the main concern in the context of e-voting. The reason for protecting secrecy is not only to protect citizens from prior intimidation or later reprisal but also to preserve a space for independent consideration about the choice.

[55] The requirement for secrecy responds to two potential risks: a) the cast vote should not be an object of control of political opinions through public authorities or others, b) no person should know how a voter intends to vote or/and has voted [2].

E-voting should be organized in such a way as to exclude anything that could endanger the secrecy of the vote (CoE Standard No 16). The secrecy of the vote, physically protected by traditional voting procedures, has to be guaranteed during the casting, transfer, reception, collection and tabulation of e-votes. None of the actors involved in the voting process (organizers, election officials, voters, etc.) should be able to link a vote to an identifiable voter or even to a group of voters. E-voting is a unique online “transaction”, by which traceability should be excluded. There must be no possibility to reconstruct a link between the voter and the vote. A major difficulty remains that the exclusion of “traceability” should be harmonised with the need that every voter has to be identified and authenticated. This need exists in all voting systems. While, in traditional voting systems voter’s authentication and voting stage are physically and temporally separated and this separation is controlled by election officials, this tension is particularly acute for e-voting given its more stringent identification requirements[22]. Consequently by e-voting, a clear and evident separation of registration and authentication procedures and casting-transfer of the vote should be designed and provided, although the combination of secure authentication of voters and guaranteed secrecy of the vote seems to be a hard requirement to comply with [42, 32]. As additional standard aiming to preserve the secrecy, the Council of Europe recommends that measures should be taken to ensure that the information needed during and for electronic processing cannot be used to breach the secrecy of the vote: such measures could be the storation of the votes at random in the electronic ballot box. Proposed has been also anonymous e-voting as a mean to preserve secrecy. However, anonymous voting would breach the principles of equality and freedom: as multiple voting could be possible and it would allow the pressure upon the will of citizens, especially those, who are upon dependence[2].

The secrecy of a vote constitutes a fundamental principle, which can be satisfied through the personal and anonymous nature of the voting act [10]. As secrecy is intended to protect freedom of choice, no voter should be able to prove that he/she has voted in a particular way [25]. As the Council of Europe recites in the Explanatory Memorandum, the system should indicates clearly to the voter that the vote has been cast and the procedure has been completed successfully, “which is important from the point of view of trusting the system and because of the principle that every vote has to be taken into account” (CoE, Standard No 14). The 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 [7,41,54], but it cannot relate to the content of the vote [15]. Excluding the individual verifiability [1] of the vote casting process may appear - in view of the potential of new technologies - as a restriction of voters’ options, but in fact it constitutes a protection against undue influence and practices like vote selling [32]. It is argued that the absence of more detailed receipt rules out an alternative control with traditional methods and therefore the system’s reliability depends on the internal computer protocols [4]. Undoubtedly, this particular question indicates how difficult it is to reconcile secrecy on the one side and transparency, auditability and verifiability on the other.

Secrecy is predicated on voting being a private act in which the individual, in isolation and free from the immediate influence of others makes up his/her political choice [30]. Coercion in workplaces or homes cannot be excluded. In workplaces, even if the employer, the supervisor, or the colleague are not looking over the shoulder of the employee-voter, intranet system administrators may monitor or record the activity at each workstation and obtain a copy of the ballot [25,27]. Although there are technological means to protect the secrecy of the ballot could be available, the level of IT literacy necessary to download and install anti-surveillance software may well prove beyond the capacity of the vast majority of the voters [22]. An additional concern refers to the risk, that some employers might be minded to take punitive action against the employee to vote for a party or a candidate not favoured by the employer. [55] Since the employment relationship is not balanced, it is therefore suggested to avoid or even to forbid e-voting from the workplace.

But also “home voting” and the preservation of secrecy and freedom seem to be contradictory in terms [54], taking in account the spatial and social dimension of home voting but also the digital divide between generations: if the main risk consists in pressure upon voters being compelled by a parent or a spouse to vote in a particular way, another conceivable scenario is a household that gives all its PIN numbers to the computer literate minor, who casts the votes for the whole family [23]. The French Data Protection Authority (CNIL) has issued negative opinions on three cases where local authorities requested permission for experimental electronic voting through Internet for (a) the Presidential Election (CNIL, Délibération 02-022 du 2 avril 2002), (b) the election of local councilors ( CNIL, Délibération 02-090 du 28 novembre 2002) and (c) the election of magistrates in labour tribunals ( CNIL, Délibération 02-091 du 28 novembre 2002). The French Authority’s opinion was based on the fact that there was no sufficient guarantee of secrecy and privacy before and during the electoral process, nor satisfactory possibility for effective administrative or judicial control [10].

These phenomena could not only violate the principles of secrecy and freedom but furthermore jeopardize the integrity of an elections outcome. It is an inherent risk of any form of remote voting. An argument against the abovementioned concerns the convenience that e-voting offers to the majority of the voters. Why should a minority prevent the majority from taking advantage of an improvement? Such an argument could not be acceptable taken into account the constitutional law in most countries as well under the provisions of the Third Article of the First Protocol to the European Convention on Human Rights. Secrecy is paramount and there is no room for derogation. [55]
There can be no guarantee of the freedom from external influence by third parties during the casting of votes. On the other side, the evidence to date indicates that postal voting, another form of remote voting, does not pose problems to the extent that it undermines the integrity of the ballot. This is especially pertinent to Europe, which has a long tradition, and history of postal voting that has been operated successfully for many years across States. Coercion and influence can hardly be prevented by technology. Keeping e-voting as a supplementary option to traditional voting, as well as making available publicly accessible infrastructure, in sites monitored by public officials, allow voters to exercise their rights free of coercion of a third party [31], without excluding that some voters may be forced to choose e-voting and vote in a particular way. To cope with this risk, measures should be taken on policy and regulatory levels, in order to impose compelling and enforceable measures against coercion and to sanction illicit behavior, without underestimating the difficulty of enforcing the law: if a person lives and votes under pressure at home or is dependent on his/her monthly salary it is wholly unrealistic to expect him/her to make a complaint of a corrupt electoral practice [55].

4.4.3. Secrecy, data protection and confidentiality

Breaches of secrecy constitute not only a violation of political rights but also an infringement of personal freedoms and privacy rights. Privacy is not simply a refuge for individuals but an expression of self-determination and a prerequisite for the capacity to participate in social and political discourse [48]. Informational privacy is an integral part of the political process. Deliberative autonomy, meant as the underlying capacity for decision-making, plays a critical role in promoting deliberative democracy [46].

Political privacy [17] pertains not only to the requirements of secrecy, as analyzed above, but also to the use of data produced by e-voting procedures. In this respect, every processing of voter data during an election procedure should be conceived and organized in a way that privacy and confidentiality are preserved and guaranteed and the respective legislation, if any, is respected. It is worthy to point out that the Council of Europe in the draft recommendation seems to perceive privacy and confidentiality as a part of security standards (CoE, Standard No 78) and not as matter of secrecy.

A first issue concerns the use of voter registers. Parties and individual candidates actively seek voter registers for a number of reasons, such as campaigns. Election data would undoubtedly be very valuable for political consultants, election system vendors and marketing firms [25]. Besides, some legislations explicitly allow or implicitly tolerate the practice of selling electoral registers to direct sales companies, credit reference agencies, charities etc. [54]. In our view, personal data and especially those relating to participation and electoral behavior, such as data necessary for registration, authentication or verification of calculation, should not be considered as a simple source of revenue for authorities [19]. These practices infringe Article 3 of the First Protocol and Article 8 of the European Convention of Human Rights. [32]

The Hellenic Data Protection Authority [HDPA] was asked about the amount of data that should be submitted to the local authorities in order for them to compile the electoral rolls and issue the voters’ booklets which ceased to exist in the meantime.
Based on the principles, that the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed, the Hellenic Authority excluded the recording of the subjects’ spouse’s name, profession and home and work telephone numbers as exceeding the purpose of the processing (HDPA, Decision no 1123/27.9.2000). In another decision the GDPA stated that a consequence of transparency and publicity of the electoral rolls is the legitimate interest of any voter to check their accuracy and exactness. Such interest obviously supercedes any right or interest of a person the name of whom is listed in the roll (HDPA, Decision no 60/2002). The necessity of the smooth running of democratic procedures was the grounds for allowing candidates for elected public offices (MPs MEPs, Mayors, Prefects etc) to collect personal data from publicly available sources and process them without being necessary to inform the subject (HDPA, Decision no 11/2001). [20]

In addition, personal data related to, needed for or produced by election procedures must be used only for the defined purpose, i.e. for organizing and holding elections, and in a way compatible with this purpose [12,34]. Unauthorized transmission or disclosure of personal data to third parties is not allowed. Data collection and processing are subject to constraints, derived from the - worldwide, even with great discrepancies - admitted principles of finality and proportionality. Unauthorized access and secondary use of data may restrain voters from exercising their rights and consequently pose a threat to democracy. From the finality principle we can derive the obligation to take all technical measures, in order to anonymize all data that relate to an identified or identifiable voter, as soon as the objectives of their processing, including verification and control of the procedures, have been achieved. The proportionality principle imposes the processing of data, which are adequate and relevant for the e-voting procedures and they are not excessive with respect to this purpose. The French CNIL put special emphasis on the respect of the finality principle as well as the proportionality principle [29]. CNIL has expressed the opinion that such e-voting procedures fall into its full competency realm and the control. At this point a strong overlap between data protection legislation and several constitutional clauses and respectively a strong overlap of competencies between Independent Data Protection Authorities and election officials could be raised.

Specific issues are raised in connection with the use of sniffing software (or hardware), which permits the monitoring of traffic on a network: the data controller, in our case the election authorities, should take all necessary measures to prevent such a use. For the same reason, the use of cookies on polling sites should strictly be prohibited, taking into consideration that it may reveal personal information related to the e-voting procedure. Furthermore, concerns are expressed with reference to the use of mobile phones as a means to exercise voting rights: special legal measures should be taken in order to guarantee the confidentiality of voting data as well as of traffic and location data, not only for the authorities involved in an e-voting process but also for the providers of WAP (and similar) connections [32].

4.5. Direct suffrage: Consequences and requirements

The principle of direct election ensures that there can be no intermediaries in the process of voting decision. Therefore, there can be no interim stage (between the voter, the voting procedure and the counting of votes), in which a third party may
This principle may be well adapted to fit an e-voting procedure. According to the Council of Europe the principle of direct suffrage does not call for special attention and is therefore not addressed in the (draft) Recommendation. The relevant requirement is that each and every online ballot is directly recorded and counted. A problem may arise in case that the voting period differs from 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 for the recording and maintaining of the cast vote, while prohibiting any counting before the end of the (off-line) voting period. [19]

5. Procedural safeguards and/or democratic requirements?

Elections are political events and e-voting constitutes a new mode of participation in political processes. Legal requirements are necessary but not sufficient to respond to the issues raised through the introduction of e-voting process. “Procedural safeguards”, as defined by the Council of Europe, should ensure that all principles of democratic elections and referendums are implemented and maintained in an e-voting context. Evolutions and innovations of voting systems must be evaluated on the basis of democratic criteria including transparency, controllability, accountability and - last but not least - legitimacy.

5.1 The transparency and control element

5.1.1 Transparency

A key element of democratic, free and fair elections is the trust and legitimization that is gained by having a transparent vote casting and counting procedure. 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 cast and counted in the presence of the parties’ representatives. Openness is lost in online voting procedures: Electronic voting machines are completely closed [8]. Many of the processes are not visible: “one cannot see the voters … nor their names being marked on the register. One cannot see the ballot boxes being sealed … or the ballots being counted into piles” [51]. Ballot counting in public is among the factors which foster trust in the procedure [33]. This inherent distrust in an e-voting procedure is related also to the digital divide [37, 47].

It should be noted that the level of trust and public support for e-voting must be measured in relation to all potential voters, not just to those who are likely to utilize this form of voting. In the case of online voting, neither the average voter nor the average party representative has the knowledge necessary to understand how the system works [32]. The Council of Europe insists on the requirements that,
information on the functioning of an e-voting system should be made publicly available (CoE, Standard No 21). A further standard (CoE, Standard No 22) refers to the opportunity, that should be offered to the voters, to practise any new method of e-voting before and separately from the moment of casting an electronic vote.

The loss of visibility, seen as a loss of (direct) controllability, may undermine the confidence in election procedures and may result in the loss of legitimacy of the outcome. Full understanding of the e-voting system(s) in use is the basis for this confidence. Voters, parties and candidates must be ensured that there has been no malpractice. But trust in an online voting system means having confidence in the machinery and infrastructure rather than simply in the physical and administrative process [51]. Moreover, whereas traditional systems have the important advantage of decentralisation, which is a factual obstacle to large-scale fraud brake [33], online voting systems are inevitably centralised and rely on equipment handled by some experts in the absence of public scrutiny [8]. As a result, in the case of e-voting much more trust in the technology is needed, as well as in the roles and characteristics of the persons involved (election officials, technology providers, etc.) [17, 27, 32].

5.1.2. Control and verifiability

Because voting is a public good, public control is essential. The regularity of the voting procedure, as well as the control of this regularity, is decisive and irreplaceable element of democratic legitimization [3]. The regularity of elections must not only be affirmed by specialists but should also be confirmed in a way that creates public confidence. Openness must be preserved and encouraged [8]. All operations (authentication, vote recording, tabulation etc.) should be logged and monitored, while secrecy should be preserved. Infrastructure and equipment should be open to inspection by authorized bodies and parties’ representatives [31].

An e-voting system should be developed in such a way as to preserve its controllability. The Council of Europe recommends that observers should be able to verify that the e-voting system itself is designed and operated in a way that respects the fundamental principles of democratic elections and referendums. Observers will thus have to be provided with an opportunity, in particular, to have access to relevant software information, to see physical and electronic safety measures for servers, to inspect and test certified devices, to have access to and test, sites and information provided for remote e-voting, and to observe cast electronic votes entering the electronic ballot box and that votes are being counted [14].

Due to the increased complexity of hardware and software the degree of controllability remains questionable. In order for the voting process to be accepted, it is absolutely essential that all the software used during the operation is not only secure but also fully transparent. Non open-source software is secret by definition and there hardly is a way for anyone to be sure that the software does not include a hidden module, which is secretly aiming at manipulating election results. The question of an open source code appears to be dealt with as an element of an open and revitalized (e-) democracy [3, 32]. In any case, critical system elements and components should be disclosed, at least to the competent electoral authorities and to observers, to the extent permitted by
the law, in order to allow them to evaluate or, if provided, certificate the system (CoE Standard No 24).

The counting procedure in particular must be verifiable, transparent and open to scrutiny. Therefore, verification procedures of the accuracy and soundness of hardware and software used for counting ballots must be provided. A recount, as well as re-production of results and procedures should be possible, in order to guarantee the accuracy of results while protecting the identity of voters and preventing the traceability of their behavior [7,43]. To verify the result, it may not be sufficient only to conduct a recount. Depending on the architecture of the system used, there may be further elements that contribute to the correctness of the result [14].

5.2. Liability

Strictly related to the issue of controllability is the question of liability. As voting systems increasingly rely on software and network technologies, it is no longer possible for election officials to be personally knowledgeable or accountable for possible failures [25]. Liability is being “transferred” to other categories of actors and its nature is deeply changing. Furthermore, the fact that in e-voting a number of intermediaries, who are mostly private companies and who are inevitably involved in a public procedure [3], is involved must be taken into consideration; this complicates the issues of liability. Even if companies providing equipment and software could be made liable and controllable through appropriate contract clauses, the liability of other intermediaries, such as access, service, and network providers, remains a problem [32]. It is interesting to note that the Council of Europe excludes the possibility that the final responsibility can for reliability and security be delegated to a voting system supplier. [14]

A critical problem is raised in relation to the nature of the network used for e-voting applications and its institutional implications. Global communication networks challenge the way interactions are regulated, implemented, controlled and the way offences are punished. The global nature of networks as well as trans-border online transactions challenge sovereignty paradigms [38] and constitute an obstacle to the control of voting procedures. The French Data Protection Authority (CNIL) has denied its “favorable opinion” to the application for trial of e-voting on the grounds that the server being used was situated abroad and was not subject to supervision by national authorities. Internet, an international medium, which is not governed by a sovereign entity [5], introduces the possibility of automated fraud and attacks that can be launched across national borders, and raises serious jurisdictional issues [25].

5.3 Reliability and security as constitutional requirements

Reliability and security requirements are derived from the democratic need to ensure that the outcome of an election correctly reflects the voters’ will. A reliable system must ensure that the outcome of the voting process corresponds to the votes cast, i.e.,
that it guarantees secrecy, equality and integrity [31]. Voting online requires a degree of security beyond the current standard for everyday Internet use [9]. Security is a multidimensional notion in the context of e-voting. It primarily refers to the (technically guaranteed) respect for secrecy and freedom, but in reality it covers the entire range of functions and election components such as registration, eligibility and authentication. The ballot being transmitted to the vote counting equipment must be an accurate and non-modifiable copy of the voter’s real choice, with no possibility of modification anywhere in the transmission path, in any of the intervening networks and devices, including the infrastructure used by the voter (integrity). This is an extremely difficult requirement to comply with, given that the opportunity for an external attack would be significantly increased, particularly in view of the vulnerability of personal computers. Security further pertains to the availability of the system and to its protection against accidental or intentional denials of service, which could result in the loss of the capability of the voter to exercise his/her fundamental political rights. [32]

The Council of Europe recommends that all possible steps should be taken to preserve the availability of its services during the e-voting process and to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process. The Council of Europe adopts a “balanced approach”: even if it recommends “that new voting channels need to be as reliable and secure as traditional voting methods”, “the recommendation is not intended to suggest that every possible method of protection available must be used in every case. In each case a judgement will have to be made as to the nature and extent of the protection measures to be applied”. The Council of Europe is aware of the difficulty to strike a balance between all-important need for security and the advisability of having usable systems and it accepts that usability, while not overriding the security, may be a factor in determining the security measures to be adopted. [14] Security aims at protecting the integrity, generality, equality, freedom, secrecy and fairness of elections. Security must of course not jeopardize the voting principles that it is called upon to guarantee; it has to comply with the requirements of transparency and verifiability. In conflict with other interests, such as the convenience of voting at a given level of technology, security remains, together with probity and accuracy, an integral component of the vitality and credibility of democracy. [32]

Some researchers and practitioners argue that there is no reason to demand absolute security, whereas this is not the case in the other voting modalities. They point out that probably there is no 100% safe solution to the complex security problems raised in the context of e-voting. [3] and this is the case also by traditional voting systems. By invoking the proportionality principle, they support “optimum security”; under given circumstances, which are necessarily subject to change, as opposed to “maximum security”[2]. If such a security threshold were required democratic decision - making processes would simply have to be abandoned everywhere in the world. Remote e-voting should, nevertheless, be as secure as possible and robust against potential inside and outside attacks, system failures, multiple voting, etc. [2]

Easier and comfortable vote has as inevitable consequence the intensification and multiplication of risks. However, security is not a purely technical, but a political issue as well. Facing the problem of security demands undoubtedly in the final
analysis a political choice: how much security can and must be guaranteed at a given moment in a given context without threatening or even sacrificing advantages of e-voting? [3]. However, we cannot ignore that a threat to security would undermine not only the public trust in and the democratic legitimisation of elections, but also the election process as such, with wide-ranging institutional, political and economic implications [42]. Security and confidence are not only means of making elections secure, but also means of convincing citizens that the system is secure [30]. The citizens must be informed about the inevitable lacks of security, bearing in mind that is a matter of the function of democratic institutions and not a pure choice of any particular citizen to vote in a not absolutely secure way. Furthermore, citizens must be involved in the discussion, in order to be able to take an informed decision and support political choices about the level of security to be provided. [32]

6. Some concluding thoughts

Changes must be assessed and evaluated on the basis of criteria embedded in democratic constitutions and liberal political culture: equality, freedom, transparency and accountability. E-voting will only be acceptable for citizens if the process is designed in such a way that it safeguards these principles. Compliance with these standards is an important element in enhancing the democratic quality of the e-voting system but alone it does not guarantee the democratic quality of the e-election or e-referendum. The e-election or e-referendum has to be judged as a whole and in detail, in the specific context [14]. We should resist changes that would fail to achieve public confidence or to meet the highest democratic standards. Unequal access to ICT infrastructure and capabilities remains a crucial problem to solve, in order to enable all citizens to have an impact on political life and to avoid a re-construction of new political elites and a “restoration” of (aristocratic?) “two-thirds democracies”[32].

Plans and discussion about e-voting reflect the tendency towards the establishment of a modern formation of public and private life/sphere, where people substitute physical participation (to events) with using communication means [5, 51]. Exercising political rights gradually loses its social (and perhaps also democratic?) nature in favor of an individualistic perception of life, which is a common characteristic of the overall social phenomenon [2]. However, democracy is not simply a matter of convenience: As e-voting is not merely a logical extension of everyday transactions and Internet applications in commerce and government [9,25], but a way to exercise a political right, deeply embedded in democratic traditions and constitutions, its introduction and acceptability depends upon its ability to respect, safeguard and promote the principles pertaining to this, most decisive, component of democracy.

Technology could and should serve as a means of coping with the crisis of participation and confidence that democracy is facing in our days [10, 32]. It could serve towards making democracy more accessible to citizens. E-voting can increase the quantity of participation. But it is not a panacea; perhaps it can “provide a crucial opportunity for the reorganization of the public sphere” [53] but it cannot itself revitalize democracy and redress the drift, just as convenience and “mouse-click voting” cannot replace participation.
REFERENCES

5. Bundesrat (Schweiz), Bericht über den Vote électronique – Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte.
13. Council of Europe – Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical Standards for e-enabled voting, Draft Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, (July 2004)
19. e-vote: An Internet based electronic voting system, Legal and regulatory issues on e-voting and data protection in Europe, EU-IST-2000-29518 (D. 3.4.).


52. The Legislative Assembly for the Australian Capital Territory – Electoral Amendment Bill 2000 No. 2 – *Explanatory Memorandum*.

