Aspects of Regulatory and Legal Implications on evoting

Athanassios KOSMOPOULOS*

Contents

Ⅰ. Introduction
Ⅱ. e-Voting definitions
Ⅲ. Election Principles
Ⅳ. Analysis of election principles
Ⅴ. Direct Democracy vs Representative Democracy: Main Issues
Ⅵ. Conclusions

Abstract

This paper addresses the democracy-oriented regulatory and legal requirements that e-democracy impacts. It demonstrates that the structure of the political system also plays a significant role in the decision to develop an e- voting application. The short term perspective of the questions put before the electorate obliterate the long term perspective in which many policy problems have to be seen. A well-designed e-voting system should produce an audit trail that is even stronger than that of conventional systems (including paper-based systems). Remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science issues are addressed. Conclusively the paper focuses on the specific attributes an electronic voting (polling place) system should respect and ensure such as transparency, verifiability, accountability, security and accuracy in relation to the constitutional requirements such as General, Free, Equal, Secret, Direct and Democratic.

* Managing Authority fort the Operational Program "Information Society"
Ministry of National Economy 105 57 Athens Greece
kosm@aegean.gr, http://www.infosoc.gr

Ⅰ. Introduction

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 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. The most powerful and politically significant aspect of new technologies is for allowing people to collaborate and self-organize: not simply the ability to reorganize the relationships between governments and citizens, but to create new opportunities for citizens to organize them selves.

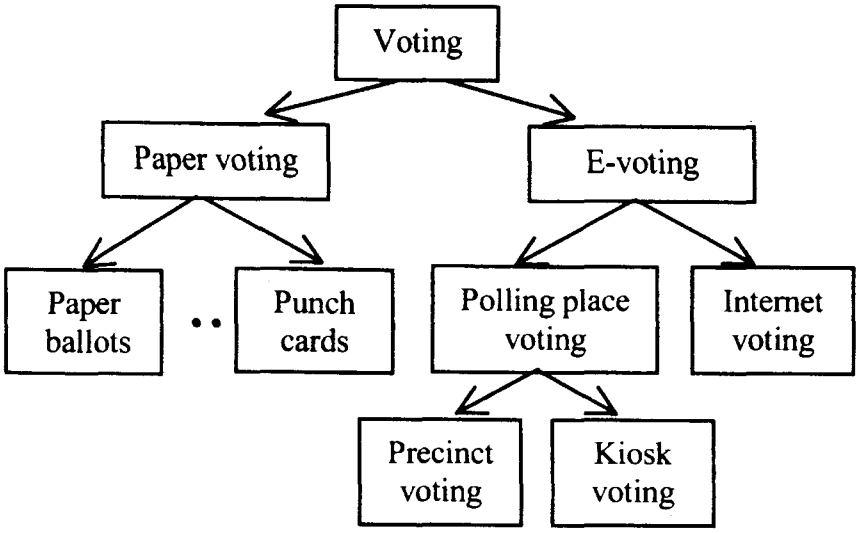
Recent reports (i.e. CalTech-MIT Report, California Internet Voting Task Force, IPI National Workshop on Internet voting, European Union IST project, SERVE project in the USA etc.) describe the capabilities of e-voting systems, and at the same time identify their limitations, the risks and vulnerabilities they are exposed to, as well as the social concerns such systems give birth to.

Despite the large volume of material published to support this debate, including several user requirements specifications, to the best of our knowledge no consolidated view on the requirements deriving from constitutional and legal consideration is available. These requirements and needs describe and identify the reflecting technical requirements that a voting system should comply with. This is the main contribution of the paper. The paper is structured as follows: In section 2, we exhibit the definition of e-voting with respect to voting technologies and processes. Section 3 presents the main election principles. Section 4 discusses in depth details of the legal and constitutional requirements an e-voting system should respect, stemming from the democratic nature of the election process. Section 5 demonstrates the most important trends of direct democracy. Finally, section 6 summarizes our conclusions.

Ⅱ. e-Voting definitions

For the purpose of this paper we define e-voting as the use of a digital or analogue device, within a secure, authenticated environment, to cast a vote during an election process. We will consider both "voter present" and "voter non present e-voting" denoting whether the voter is physically present in the polling booth or remote from it. Electronic voting (e-voting) uses digital data to capture the voter selection. With Internet voting (I-voting) the voter casts his vote remotely via the Internet.

Fig. 1. Types of Voting



2.1 Voting technologies and processes

There are five broad classes of voting technologies in use today [1] throughout the world:

- Hand counted paper ballots
- lever voting machines
- punched card ballots
- optical mark-sense ballots
- direct-recording electronic voting machines

A variety of voting processes are employed throughout the world. The most common is traditional voting at the poll site on Election Day. However, there are several alternative methods, including:

- Absentee ballots: Is the provision for the use of absentee ballots, which allow people to vote-by-mail before the election. Many countries provide absentee ballots only to those people who certify that they are unable to get to the polling place on Election Day, for such reasons as travel or disability. Other countries provide absentee ballots to any registered voter who requests one.
- Vote-by-mail: According to the Dutch law, only voters who reside outside the Netherlands, or live outside the country due to their professional activities, or because of their marital partners or their closest relatives are allowed to vote by mail. In Germany postal voting is allowed if only if the eligible voter applies for this option on important grounds as for illness, absence which prevents him from voting in his electoral district during voting day and

hours. Oregon is the first, and so far only, state in the USA to adopt all mail voting [2]. Oregon mails ballots to all registered voters, who generally return the filled-in ballots by mail. There are no longer any traditional polling places, although each county provides booths where people can fill out their ballots in privacy and places where they can directly deposit their ballots. Most election jurisdictions have not adopted vote-by-mail and restrict the use of absentee ballots, in part because of security concerns. With absentee ballots, a person can be observed filling out the ballot, and there is a greater possibility for a person to sell their vote or to be subject to coercion. There is also no timely feedback to indicate whether a mailed ballot has been received by election officials in time to be counted.

Recently the significant report EVE [3] has shown that Internet voting is mostly being considered by countries that have already implemented changes regarding the polling methods, such as:

- placing electronic ballot boxes in polling stations,
- introducing postal voting,
- using the Internet as political campaign tool.

Remote voting where voters are not constrained to vote at designated precinct polling places on election day is largely a matter of law but it relies on many enabling technologies. Remote voting on election day is sometimes described as the vote anywhere model. In this model voters may use any polling place, however it was eliminated by its high susceptibility to fraud, nevertheless the combination of smart cards, biometrics and highly available on line voting systems may allow such a system to re-emerge. The arguments of the California Internet Voting Task Force against Internet voting on election day apply to most versions of the vote anywhere model so there is good reason to be skeptical about such systems [4].

There is concern in many democracies about the declining rates in voter turnout and more generally, the apparent tendency towards political apathy. To reverse this, and to promote political activity, political reform is needed. One of the measures considered is to simplify the election procedure by introducing electronic voting, and in particular Internet voting. It is expected that this will increase voter convenience and voter confidence in the accuracy of election results. In the context of our analysis we make a distinction between two types of e-voting: polling place voting and Internet voting and furthermore we distinguish two types of polling place voting, namely precinct voting

and kiosk voting. In this paper we will focus mainly in polling place e-voting and not particularly in Internet voting. (see fig.1)

In polling place voting, both the voting clients (voting machines) and the physical environment are supervised by authorized entities (closed regulated environment). Depending on the type of polling place (precinct or kiosk), validation may be either physical (e.g. by election officials) or electronic (with the use of digital identification). Casting and tallying of votes are electronic: the voting clients may be Direct Recording Electronic devices (DRE' s) or they may send their tallies electronically to a central site (e.g. by using, a dedicated line or an ATM network).

Ⅲ. Election Principles

Generally speaking, each election involves four distinct stages:

- Registration

Prior to the election, voters have to prove their identity and eligibility. An electoral roll is created.

- Validation

During the election, voters are authenticated before casting their vote. Only one vote per voter is authorized.

- Casting (Voting), Voters cast their vote.
- Tallying, At the end of the voting period, all votes are counted.

Each of the above stages can take place by using *physical* or electronic procedures.

Any technology used in the context of an e-vote process must meet a set of fundamental constitutional requirements. It is generally 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 main European Union member states demand that the parliamentary elections must be General, Free, Equal, Secret, and Direct. Adding up to the aforementioned elements the essential requirement of Democracy, and analyzing these requirements to the next level of detail we get hold of the first-level legal and regulatory e-voting requirements, which are summarized as follows [5] :

Table 1. First-level legal and regulatory e-voting requirements

1	General
	1.1 Universal opportunity to participate
	1.2 Eligibility (registration and identification)
2	Free
	2.1 Uncoercibility
	2.2 Eligibility (registration and identification)
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

Ⅳ. Analysis of election principles

4.1 General

Universal involvement is a basic principle for democratic elections. According to this constitutional requirement, every eligible voter may participate in the election process. No one can be – directly or indirectly – excluded or discriminated. The main consequence deriving from the principle of general elections is that every voter has the right to participate in an election process while the ability to participate to this process (eligibility) must be founded on the law and should be regulated according to the law. This requirement responds to a constitutional requirement embedded in many constitutional texts.

Furthermore, voting possibilities and technologies should be accessible by every voter, whilst considering the lack of necessary infrastructure and the digital divide, e-voting should be considered only as an alternative complementary way of exercising one's voting rights.

The principle of universality requires that every eligible voter should be included in the election process, and therefore this principle results in the necessity for publicly available appropriate infrastructure (e.g. public internet kiosks, voting equipment in closed regulated areas such as government offices, etc.), in order to allow all citizens to

exercise their voting rights.

E-voting improves the generality of election procedures by providing an additional "channel" of participation in the electoral process. A critical 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 we described above.

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.

In opposition to this opinion, emanating from the historical and legal basis that voting in a physical voting station constitutes the rule, the following argument may be articulated: the evolution towards an information society has a significant impact on the ability of a citizen to exercise his/her rights and liberties. Having in mind the political decision to improve e-government and e-democracy, the introduction of an e-voting capability should be viewed as an institutionally equivalent and not as an exceptional and complementary option.

Eligibility initially, can be guaranteed through the registration of voters, who meet the specific requirements of eligibility, and on a second phase through the identification of the citizens at the moment of registration. (Secure) Registration and authentication (identification) are the means to ensure that the principle of universal suffrage is being respected and that elections cannot be influenced.

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 a functional way, 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 [6].

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.

A voter registration system must meet five standards [7].

First, registration information must be accurate and complete. The information on the voter registration rolls must cover all registered voters and have the correct information used to authenticate the voters, that is, to verify that the voter is eligible to vote for a prescribed set of races.

Second, registration information must be immune from fraud. If the aim is to prevent fraud, then it should be difficult or impossible to create fraudulent registrations.

Third, registration information must be dynamic and up-to-date. Voter registration must be flexible to accommodate frequent moves made by previous voters, the addition of new voters, and late voter registrations. Registration must also fit with election schedules. A significant challenge is developing a fraud resistant system for last-minute registrations, including Election Day registration.

Fourth, registration information must be usable by the election officials at the polling places. Because election officials use this information to authenticate voters, polling place workers must have usable registration information.

Fifth, it must be easy for voters to register. Registration should not be a burden to voters.

Finally 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.

4.2 Free

The principle of free elections requires that the whole election process takes place without any violence, coercion, pressure, manipulative interference or other influences, exercised either by the state or by one or more individuals. In many countries, regarding the postal voting case, the 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.

However, e-voting procedures in open non regulated environments (such as Internet) 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. Moreover, the distributed nature of the Internet could facilitate large-scale vote

selling or trading [8]. We suggest, as we will explain later, that the best solutions are voting systems exhibiting a "voter-verifiable audit trail," where a computerized voting system might print a paper ballot that can be read and verified by the voter [9]. However this paper "receipt" must be placed in a sealed box by the voter at the designated polling place, in order to prevent vote selling, intimidation or other coercion instances. These paper receipts may be used as well for additional recounts if such a need occurs.

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). In any case, coercion can hardly be prevented by technology alone. A possible solution is to develop a public accessible infrastructure, in closed regulated 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 voting equipment, 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 equipment.

The requirement of equality in the context of public elections is a specific expression of the legal principle of equality. It constitutes one of the political cornerstones of modern democracies.

A blank vote is defined as a vote where the voter does not designate any candidate. During a paper vote, blank votes are usually counted as cancelled votes and cannot be distinguished from invalid ballot papers.

The question of knowing whether blank votes should be officially taken into consideration is, what' s more, a matter for debate. For political elections in France [10], a recent bill was aimed at enabling blank votes to be precisely defined and to be distinguished from invalid ballot papers.

Nevertheless, some people believe that recognising a blank vote would be liable to falsify election logic due to the possibility of voters casting a vote of no confidence rather than a positive choice.

This democratic debate exceeds the aim of this paper. At this stage, it is only necessary to note that a decision to count blank votes would be facilitated by the introduction of electronic voting systems.

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. In order to preserve the freedom of voters' decision, the possibility for casting a

consciously invalid vote should be provided and guaranteed.

4.3 Equal

The requirement of equality in the context of public elections is a specific expression of the legal principle of equality. It constitutes one of the political cornerstones of modern democracies.

The principle of equal suffrage is identified mainly in equality regarding the candidates and the political parties who participate in the public elections.

A requirement deriving from the principle of equality is that electronic ballots should be edited and displayed in a way similar and equivalent 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 e-voting equipment (i.e. on the screen of the e-voting machine) should ensure equal accessibility. Thus, the structure and appearance of ballots should not favor or discriminate against any of the participating parties.

Another aspect 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. This is a matter of security which will be analyzed on the sequel.

Transparency should also be respected. 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 other side of equality is the one regarding the voting rights of each voter.

In view of the current technological and societal evolution, 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. 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). Digital and technological divide is a major issue in this context.

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 "duplicability" of the vote (either by

the voter her/himself or by someone else);

- the "reusability" of the vote (either by voting more than once online or by voting both online and offline);
- the "alteration" of the cast vote (after a voter has dispatched her/his vote).

4.4 Secret

If Secrecy and freedom are strictly related principles: Secrecy is the prerequisite of the voter' s free political decision. In democratic elections the connection between the vote and the voter must be unachievable, 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.

Secrecy and anonymity of the ballot also provide important checks against coercion, against a person being forced, lured or intimidated into voting one way or another by others.

The following requirements are resulting from the principle of secrecy:

The secrecy of the vote has to be guaranteed during the casting, transfer, reception, storing and tabulation of votes.

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.

There must be a clear and evident separation of registration and authentication procedures and casting-transfer of the vote.

No voter should be able to prove that he/she voted in a particular way.

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".

Secrecy has to be in accord with the other democratic principles for public elections. Ballot secrecy should be reconciled with transparency and auditability of the entire voting process. This is the main difficulty, that is to say 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. Universal verifiability is the case where any observer can be convinced that the election is accurate and that the published tally is correctly computed from votes that were correctly cast. Atomic verifiability is a weaker version of universal verifiability in which voters can only check their own votes and correct mistakes without sacrificing privacy. The later is useful when the cost of

achieving universal verifiability outweighs its benefit.

4.5 Direct

The principle of direct election states that there can be no mediators in the process of voting decision. This principle may be well adapted to match an e-voting procedure. The appropriate 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) conventional voting period.

4.6 Democratic

A democratically designed and deployed e-voting procedure should, at least, exhibit the requirements of a traditional election system. However, additional requirements must be also met, particularly due to the intangible nature of e-voting. These requirements relate to the preservation of attributes and characteristics, 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 as well as understandable 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 other hand, 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 verifiable by voter itself (individual-atomic verifiability) or by election officials, parties, independent observers (institutional-universal verifiability). 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 controversial 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. Extensive testing is needed despite the fact that the operational aspect is never 100% guaranteed. A Provocative Scenario [11]: A programmer at SlickVotingMachines Corp. adds malicious code to a DRE (Direct Recording Electronic device) machine for the California 2004 Presidential election, so that every fiftieth vote for a Republican candidate is changed to a vote for the corresponding Democratic candidate. This only happens when the machine is in "real" mode as opposed to "test" mode, so the election officials never discover the fraud during their testing. The electronic audit trail made by the DRE machine is also affected, so "recounts" never discover anything amiss.

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

Based on the above principles, the following, functionality-oriented, requirements are consequential:

First of all there must be trusted certification procedures for hardware and software, while the entire infrastructure (including source code), as well as every system functionality, must be logged.

On the other hand all operations (authentication, vote recording, vote tabulation etc) should be monitored, while secrecy is preserved.

At the same time, the infrastructure should be open to inspection by authorized bodies, as voters, parties and candidates must be ensured that there has been no malpractice. Finally adequate system security must be ensured whilst the system must be simple and user-friendly.

Reliability and security requirements are based on the democratic need to ensure that the result 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 stored to the voting counting equipment must be an accurate and unmodifiable copy of the voter's real choice (integrity). Moreover, it should be impossible both to eliminate a valid vote from the tabulation, and to validate a non-valid one.

Security is a multidimensional notion in the context of e-voting.

Election principles "in toto" are safeguarded by security. As far as security is concerned, on the ground of this analysis, regarding a specific e-voting system, it must cover globally the following attributes [12] that we highlight as a set of overlapping characteristics:

- Accuracy, also referred to as correctness means that no one can change anyone else's vote (inalterability), all valid votes are

included in the final tally (completeness) and no invalid vote is included in the final tally (soundness).

- Democracy, is safeguarded if only eligible voters are allowed to vote (eligibility) and if each eligible voter can only cast a single vote (unreusability).
- Privacy, states that nobody should be able to link a voter's identity to his vote after the latter has been cast.
- Robustness, guarantees that no reasonably sized coalition of voters or authorities (either benign or malicious) may disrupt the election. (it should also be provided against external threats and attacks eg denial of service attacks etc)
- Verifiability, implies that there are mechanisms for auditing the election in order to ensure that it has been properly conducted.
- Uncoercibility.
- Fairness, this property ensures that no one can learn the outcome of the election before the announcement of the tally.
- Verifiable participation, often referred to as declarability, ensures that it is possible to find out whether a particular voter actually has participated in the election by casting a ballot or not.

Security finally refers to the (technically guaranteed) respect of secrecy and freedom but it covers the entire range of functions and election phases 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.

V. Direct Democracy vs Representative Democracy: Main Issues

The main weaknesses of existing democratic arrangements in most countries are that members of the representative assemblies represent partisan interests under the guise of the general interest.

Often they tend to follow only their own partial understanding of what is good for their constituencies, and they are more responsive to the requirements of the political party they belong to, than to the citizens whose mandate they have received [13].

The growing popularity of referenda, co-production of policies and interactive policy-making, underlines that people prefer direct democratic arrangements for the existing representative arrangements.

Representative democracy was deemed to be necessitated by the impossibility to realize direct democracy, by giving all citizens an equal opportunity to participate in the collective decision making process.

Conversely, major disadvantages on the subject of direct democracy are observed. More specifically:

- Direct democracy would lead to a single issue approach. Successive majorities on single issues would lead to incompatible policies within and between sectors. The complexities of policies require intermittent and iterative decision cycles, which are not feasible through referenda.
- Most political problems cannot be reasonably approached with a simple "yes" or "no", as opinion polls and referenda do. Besides, the short term perspective of the questions put before the electorate obliterate the long term perspective in which many policy problems have to be seen.

In this light "push button" democracy is considered fragmentary as well as showing a deficit compared to representative democracy.

On the other hand the transparency of public administration in the information society, which results from the development of ICT applications, as analysed above, forces us to re-conceptualize the democracy theory [14].

To many people the mention of e-Democracy conjures up visions of electronic polling stations and on-line referendums, but whilst these may have a part to play in the future, a more pressing objective is to maximise the opportunities for public participation in governance.

The Internet certainly isn' t a panacea, but does have the potential to bring together large numbers of people in a form of civic dialogue. It can also provide immense stores of information for people to access and interact with.

Importantly, if universal access is achieved, it allows those with few resources to have equal opportunities for political debate and involvement.

The fundamental challenge of e-democracy is to improve and develop representative democracy towards processes based on the empowerment of citizens [15].

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:

- The digital divide and
- The intrinsic distrust in an e-voting procedure [16], considering that while computer scientists, for the most part, have been warning of the perils of such action, vendors have forged ahead with their products, claiming increased security and reliability.

Relations between members of the public and holders of political authority are being transformed. New expectations and meanings of citizenship' are being entertained and occasionally acted upon. People often expect to be heard and heeded on more occasions and matters than the ballot boxes of Polling Day can settle.

Electronic voting (e-voting), as we already mentioned, uses digital data to capture the voter selection. With Internet voting (I-voting) we also get remote connectivity via the Internet. A few Internet-based elections have already taken place [17], while pilot elections are scheduled in several countries.

The most famous project is (was!) the SERVE voting system (Secure Electronic Registration and Voting Experiment), an Internet-based voting system being built for the U.S. Department of Defense's FVAP (Federal Voting Assistance Program). A very important report [18] was published according to which:".. because SERVE is an Internet- and PC-based system, it has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc.), any one of which could be catastrophic" . The report finally recommends *" shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear."* SERVE has eventually been cancelled by the Department of Defense.

Ⅵ. Conclusions

This paper intends to limit the analysis to political voting and local or national elections or referendums.

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. Therefore, 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 re-construct new political elites.

The next step beyond poll site voting would be to deploy kiosk voting terminals in public places. This path toward greater convenience would enable technologists and social scientists to address the many issues that confront the voting process at each level of implementation.

Many issues related to kiosk voting, such as setting standards for electronically authenticating voters, still need to be resolved.

Remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science issues are addressed. The security risks associated with these systems are both numerous and pervasive, and in many cases cannot be resolved using even the most sophisticated technology today. Nevertheless, it is advisable to replace punch cards, lever machines, and older full-faced DREs (Direct Recording Electronic devices) with optical scanning systems that involve counting ballots in precincts, or with any electronic technology proven in field tests.

As with other activities, the vote is currently being won by new technologies and dematerialisation.

This aim of this paper was to clarify the main legal concerns involved in electronic voting and to show that this system of voting could be introduced into the electoral process following a gradual and reasoned approach.

The introduction of information and communication technologies (ICT) into

voting operations does, in fact, considerably simplify the polling procedure, in particular, by making it faster and more functional. It echoes the increasing use of the internet in our society. Electronic voting alone will not, however, change citizens' political attitudes. It, alone, will not be able to combat the growing disinterest of the latter with regard to the polls.

On the other hand, it would appear that ICT offers individuals new forms of expression and participation (discussion forums, debates, chat rooms, on-line public surveys etc.) which may motivate them to have more of a presence in local debates and to be more active in public or private decision-making.

The 'democratic' contribution of information and communication technologies lies as much in the latter as in electronic voting.

Alternatively, security models such as the voter-verified audit trail allow for electronic voting systems that produce a paper trail that can be seen and verified by a voter. In such a system, the correctness burden on the voting terminal's code is significantly less as voters can see and verify a physical object that describes their vote. Even if, for whatever reason, the machines cannot name the winner of an election, then the paper ballots can be recounted, either mechanically or manually, to gain progressively more accurate election results.

Traditional voting systems are not perfect. In the US 2000 elections, a large number of residual votes (under votes, spoiled votes, uncounted votes, etc) were cast. E-voting promises to ameliorate this error rate substantially. It also promises to improve accessibility for disabled voters. Furthermore, election results will be calculated quickly and efficiently, with less chance of human error, and long-term costs will be reduced by eliminating the expense of printing ballots.

On the other hand e-data is likely to be more easily altered or destroyed than physical ballots. In addition, all kinds of e-voting systems are susceptible to a certain extent to insider attacks and Denial of Service (DOS) attacks. It is widely known that current e-voting systems have poor audit trails. Even worse, although there are strong cryptographic algorithms we do not have systems (e.g. platforms, operational systems) with adequate security into which the cryptography can be embedded.

Our future work will be focused in examining the Kiosk voting methodology, from the Technolegal point of view, as being the necessary phase between the polling place voting and the Internet voting. In info- Kiosk schemes, voting machines are located away from traditional polling places but under the control of election officials and also be appropriately monitored in order to meet security and privacy requirements as well as to prevent

intervention (i.e. coercion).

A well-designed e-voting system should produce an audit trail that is even stronger than that of conventional systems (including paper-based systems). Future of e-voting systems will exploit current technologies and tools including smart cards, biometrics (e.g. voice, fingerprint, retinal recognition - for identification), as well as mobile voting clients (e.g. hand-held organizers, cell phones, etc).

Research is needed to determine to what extent such technologies are viable for e-voting.

References

1. Jones .D.W. Counting Mark - Sense Ballots - Relating technology, the Law and Common Sense, January 2002; http://www.cs.uiowa.edu/~jones/voting/optical/
2. Internet Policy Institute, Report of the National Workshop on Internet Voting, March 2001
3. (《Evaluating practices &Validating technologies in E-democracy》, www.eve.cnrs.fr/)
4. Final Report of the California Internet Voting Task Force , California Secretary of State, January 2000
5. Electronic Voting : Constitutional and legal Requirements and their technical Implications, Lilian Mitrou, D. Gritzalis, S. Katsikas, G. Quirchmayr , in "Secure Electronic Voting" 2003, Kluwer Academic Publishers.
6. "Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented until an adequate authentication infrastructure is available and adopted". Internet Policy Institute, Report of the National Workshop on Internet Voting: Issues and Research Agenda, March 2001.
7. California Institute of Technology - MIT, Voting Technology Project, Voting: What is, What could be, July 2001.
8. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), January 21, 2004, Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner,
9. "Analysis of an Electronic Voting System" TADAYOSHI KOHNO, ADAM STUBBLEFIELD, AVIEL D. RUBIN, DAN S. WALLACH ,Johns Hopkins University Information Security Institute Technical Report TR-2003-19,

July 23, 2003.

10. WHAT IS THE FUTURE OF ELECTRONIC VOTING IN FRANCE? The Internet rights forum, Published on 26 September 2003
11. Same as 6
12. Secure electronic voting: The current landscape, C. Lambrinoudakis, D. Gritzalis, V. Tsoumas, M. Karyda, S. Ikonomopoulos, in "Secure Electronic Voting" 2003, Kluwer Academic Publishers.
13. ICTS AND THE FUTURE OF DEMOCRACY by Ignace Snellen International Journal of Communications Law and Policy Issue , Winter 2000/2001
14. Realising Democracy Online: A Civic Commons in Cyberspace IPPR/Citizens Online Research, Publication No.2 – March 2001
15. European Commission, IST 2000 Programme, The Information Society for all, Final Re port, Brussels 2000
16. Analysis of an Electronic Voting System, Johns Hopkins Information Security Institute Technical Report TR-2003-19, July 23, 2003 by Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach.
17. Examples are:
    - the Arizona Democratic party's election (legally binding), March 2000, Mohen, J., Gliden, J. " The case for Internet Voting". In Com. of the ACM, 44(1), 2001
    - the Military personnel Presidential election in the US and overseas (legally binding), 2000, Federal Voting Assistance Program. Voting over the Internet Project, www.fvap.gov/
    - the Alaska Republican party's election (non-binding), January 2000, May, P. "Alaskan Voters are Pioneers" Mercury News, Jan 25, 2000, http://www.mercurycenter.com/svtech/news/indepth/docs/vote012600.htm
    - the UK local and mayoral elections (non-binding), May 2002, DTLR News Release. "May Elections to Trial Online Voting" , 2002, http://www.press.dtlr.gov.uk/pns/DisplayPN.cgi?pb_id=2002_2003
    - Pilot schemes to test innovative voting and counting methods took place in 59 local authorities across England on 1 May 2003. Approximately 6.4 million people were eligible to vote in these pilot areas – over 14% of the English electorate, The shape of elections to come, A strategic evaluation of the 2003 electoral pilot schemes, July 2003, The Electoral Commission UK
    - In Switzerland, the first official ballot for which citizens can vote through Internet began on January the 7th 2003, in the municipality of

Anieres (Geneva) http://www.geneve.ch/chancellerie/E-Government/e-voting.html

- and more examples in UK, Practical experiences with e-voting in Council of Europe member states

http://www.praxis.ee/praxis/admin/texts/Michael.Remmert.pdf

18. A group of experts in computerized election security was assembled by the FVAP to help evaluate SERVE. Two three-day meetings were held in July, 2003 at Caltech in Pasadena, California, and in November, 2003 at Accenture in Reston, Virginia. Four members of the group of experts attended both meetings. They are David Jefferson, computer scientist at Lawrence Livermore National Laboratory, Aviel D. Rubin, Associate Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University, Barbara Simmons, a technology policy consultant, and David Wagner, an Assistant Professor in the Computer Science Division at the University of California at Berkeley. These four computer scientists published in January, 2004 a report entitled "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)" (the "SERVE Security Report").