

# AUDITABILITY MEASURES FOR eVOTING SYSTEMS

**Jordi, BARRAT I ESTEVE**, Research Group – SEJ2004-03844JURI

Constitutional Law Department, Universitat Rovira i Virgili, Catalonia / Spain

jordi.barrat@urv.net

## **Abstract**

*eVoting systems have less transparency than traditional electoral methods because an average citizen without specific skills cannot understand how they work. Since this obstacle can be overcome with complementary auditability measures, the paper will provide a theoretical framework developing the existing proposals and identifying the best options from a legal point of view. It will also analyze some real examples focusing on the legal documents enacted in four binding Spanish e-voting experiences.*

*Keywords: e-democracy, electronic voting, auditability, Spain*

## **1. INTRODUCTION.**

Although there are several democratic principles that any e-voting experience should respect, the paper will only analyze the auditability mechanisms of these systems (paper receipts, electoral boards, source code analysis, etc.). There are also other important issues like the official information that the citizenry receives, the identification procedures, the freedom, secrecy and equality during the voting's act and the social measures foreseen to reduce the digital gap (in general, Trechsel, 2005; Gritzalis, 2003), but the paper will be focused on the auditability problem. This is a key question since these electronic tools reduce the transparency and clarity of the traditional ballot boxes and each e-voting system tries to solve this problem in a different manner. I will analyze therefore the solutions provided by some specific legal statutes including these specific cases in a larger theoretical framework.

During the last years, several European countries have begun experimental e-voting projects. The aim of these initiatives has been to recollect enough data in order to decide if these new electoral procedures are safe. Anyway, some countries already accepted these methods with a binding format (e.g. Belgium) and others, like Spain or France, are now beginning to accept binding e-voting experiences after a period of pilot essays. In these cases, it is compulsory that the Parliaments, or other competent bodies, pass detailed Acts. Since they are not pilot elections, the citizens have the right to have an electoral legislation with a complete translation of the technical guarantees of electronic voting to a specific and normal legal language.

This is not an easy task because electoral legislations have to be very accurate since they are managing a critical field in any democratic system. The paper will be focused on the following four Spanish binding experiences: the Basque country e-voting Act, the internal electoral rules of the Basque Country University and the legislation passed by the Barcelona Engineering Association and by the government of Andalucia for the election of the parents boards in the regional schools.

## **2. THE AUDITABILITY PROBLEM.**

This is a central issue in any e-voting system. It has great importance itself, but other aspects of these procedures, like the secrecy of the vote or the equality among voters, depend as well on which audit measures are foreseen. Many basic electoral guarantees may be adapted to electronic procedures, but

these new systems cannot be as transparent as the current ones and these weakness should be addressed by serious control and audit mechanisms.

If we observe the current electoral models, we could distinguish two sorts of verification powers depending on the people taking part in these actions and their effects. Whereas the individual verification allows each voter to check that his/her vote has been correctly processed, the universal one affects the whole system and it intends to analyze the correct development of the overall process.

Nowadays both controls can be easily performed because the combination of very simple elements, like empty and transparent urns and opaque envelopes, allow any citizen to use either the individual or the universal verification power. These urns guarantee very fundamental principles like that a concrete vote has been correctly mixed with the others and that there are not added or destroyed votes. Once the electoral day ends, the citizen would be able to see the public tally in order to check him/herself that there is no fraud. It is therefore the voter him/herself who could do these verifications and, if it is not a normal behavior today, the important thing is that, if necessary, he/she could use these democratic powers. If there are any protests, a direct and personal control will be always feasible. Our current reliable electoral systems would maybe explain why these powers are not often used, but it will not justify an electoral model without these options.

On the other hand, traditional electoral systems guarantee as well, with the same elements, a universal verification. An isolated voter could not do it, but it would be feasible that a nationwide voter association performs a parallel tally in order to check the correctness of the official one. All these things can be done as well without any specific technical skill.

Shortly, our electoral systems create themselves citizen confidence without complementary measures. Any voter would accept the results without needing the opinion of other electoral experts. Can e-voting systems offer a similar degree of guarantees?

Of course not. These new procedures always depend, in one or another moment of their implementation, on electronic mechanisms and devices that obviously cannot offer the same simplicity just explained above. A citizen will not be confident into the system itself because he/she will not be able to understand it, at least with the same ease that he/she has in front of the traditional voting method. To believe that an e-voting machine makes a correct tally is really an act of faith because, without specific technical skills, these data are impossible to verify in a direct and personal form. Keeping in mind these important obstacles, which solutions may help the development of electronic voting machines?

### **3. THREE CASES OF SPANISH LEGAL E-VOTING REGULATIONS.**

Before answering this question, it would be useful to know something about the e-voting experiences that we will analyze below. Although the first Spanish e-voting essays began in 1995 (Arnaldo Alcubilla, 1998; Ambrosio, 1999), only during the last two or three years there has been a real increasing interest in these technologies with several binding and non-binding experiences. Since the first ones should have their own detailed legal documents trying to rule these new procedures, this paper analyzes four bills of these recent binding Spanish cases.

One of them is fostered by the Basque government, that is to say a country where there have been significant official efforts to develop electronic voting. Its Parliament, for instance, passed in 1998 the first Spanish e-voting Act that was based on touch-screen methods (Fernández Riveira, 2001). However, one of its articles empowered the regional government to decide whether to put into practice this technology and finally this system has not been used so far because some political parties did not accept it. Touch-screens do not allow, for instance, the traditional electoral mailing, including specific

paper ballots and envelopes, carried out during the campaigns and therefore the political parties did not accept a system that reduces their political influence over the citizens.

After accepting these disadvantages, the *Demotek* partnership, backed again by the Basque government itself, started the development of another method based this time on optical ballots. Although they are also electronic tools, paper ballots do not disappear and the described mailing would be then feasible. *Demotek* carried out some pilot essays (e.g. Catalonia 2003) and other binding experiences as well like, for instance, an internal election for the Bilbao Football Club (2001).

This project also includes a legal draft, discussed in the Basque parliament during the last legislative period (2001-2005), where these new optical ballots substitute the touch-screen system. This is the document that will be analyzed (Eusko Legebiltzarra, 2004).

The second example is a development of the first one since the Basque Country University used *Demotek* technology to manage the elections of its President in March 2004. There has been also a modification of its internal electoral rules in order to allow e-voting procedures.

The third case to be considered is the Board's renewal of the Barcelona Technical Engineering Association (CETIB). This body intends to represent the engineers living in this district and, according to the Spanish general legislation, its internal structure must be democratic. Despite this requirement, there have been low turnouts in precedent elections because, among other reasons, there was only one polling station, the district was too big and therefore the participation was difficult for those members not living in the main city.

The internal regulations were modified in December 2004 in order to allow the use of electronic voting procedures during the following Board's renewal in 2005. This is the legal document that will be analyzed (Cetib, 2004). Although it does not say anything, the manager of the e-voting process will be probably *ScytI*, a Catalan company specialized in these security technologies (Cetib, 2004a). It was born within the Autonomous University of Barcelona from several doctoral researches in this area and it has experience in some electronic elections (e.g. Notary elections in 2004) and consultations (e.g. MadridParticipa; vid. Barrat Esteve, 2004).

Finally, since Spanish schools have always an internal representative board for parents, the regional government of Andalusia decided last year to use electronic tools during their renewal in January 2005. Nine schools around the country were chosen for this experience (see the list in Boja, 2005: 7). Like the other two examples, since it is a binding e-voting election, the government enacted a specific legal document that includes several details for this procedure (Boja, 2005). *Indra* has been the technical partner of the project. It is a Spanish company with a large experience in electoral fields and it is now offering new products based on electronic systems. There have already been some binding experiences like the elections in 2002 and 2004 to the internal consultative board of the *Guardia Civil*, one of the two main Spanish police institutions.

Once described the four cases that will be analyzed, it is important to remember again that the paper will be only focused on auditability mechanisms since it is one of the critical elements of any e-voting system. Anyway, there are also other issues that could be interesting to know like, for instance, the measures foreseen to reduce the digital gap or the identification rules in these four different cases.

### **3. AUDITABILITY AND GUARANTEES.**

Since e-voting methods are based on computers, they cannot offer the same transparency of traditional paper ballot systems because the average citizen does not understand their internal requirements. This is not a definitive obstacle, but it is compulsory to implement enough complementary measures to create reliable mechanisms for everybody. Therefore the existence of independent audits is one of the

key elements to be found in any legal regulation, but the specific solutions will depend on each e-voting system. The chapter is divided in three sections that intend to analyze the three main mechanisms that can be introduced in e-voting systems as complementary control measures: the existence of a paper trail, the audit of the software components and the composition and faculties of the electoral board. We will analyze each item following the main distinction between individual and universal verification explained above.

### 3.1. Paper trail.

The existence of paper trails may be the easiest solution for an individual verification, but it admits different options depending on the e-voting system. We will analyze two cases: the optical ballots and the use of computers inside polling stations. It seems that the first ones, used in the two Basque examples –Basque Country University and regional electoral legislation— solve the problem, but this is not always true. Although these optical ballots allow second manual tallies similar to the current ones, this is –or this should be— only an exceptional measure. The ordinary mechanism consists in an electronic counting and the other tally is only used in front of specific claims, but not as a usual electoral solution.

Anyway, there could be specific methods in order to check that the ballot chosen by a citizen is really the correct one. The *Demotek* system, for instance, has an ultraviolet reader where any citizen can check the paper ballot before introducing it in the electronic urn (Barrat / Reniu, 2004: § 5). This is a good measure, but it is not enough because its counts do not offer any evidence about the tally carried out by the electronic urn. They are two different and isolated systems. The only guarantee for the citizen is the paper ballot introduced in the urn, but a second tally with this element is only foreseen exceptionally whereas the automatic counting should become the ordinary application of the system. The ultraviolet reader is not then an individual verification of the vote.

On the other hand, the second recount foreseen by the Basque documents was not actually a real traditional paper tally since, when doubts or protests arise inside the polling station, there would be a recount only with the mentioned reader. It describes this task as an electronic-manual tally, but this solution is not a traditional tally only with the paper ballots introduced in the urns and without any specific device. The article 132 Quinques VI.1 states that «este nuevo recuento sólo se realizará mediante el aparato comprobador de la cabina electoral. En ningún caso, se permitirá abrir las papeletas de votación electrónica, para evitar el posible deterioro de las papeletas y la consecuente anulación de votos válidamente emitidos» (this second tally will only be carried out with the checking device of the polling booth. To open the paper ballots will never be allowed in order to avoid damages and the consequent exclusion of votes correctly cast) [vid. also articles 31.5 and 31.6 of the electoral legislation of the Basque Country University (Euskal Herriko Agintaritzaren Aldizkaria / Boletín Oficial del País Vasco, 10<sup>th</sup> February 2004, p. 2653)]. If there is a claim about a specific paper ballot, the electoral board should not destroy this evidence and send it to the electoral competent body, but this second level could not again perform a traditional tally opening the paper ballot and reading its content because the legal draft only allows to check it again with the ultraviolet reader (art. 132 Sexies 4). Although the bills do not say anything, there could maybe be a different final solution in the Courts, but not inside the electoral Administration.

Secondly, e-voting systems without optical ballots can include also a paper trail if they are used inside polling stations:

a) during the last referendum in Venezuela, the machines printed a paper receipt with the political option chosen by the voter. The citizen him/herself got this document and introduced it in a traditional urn placed inside the electoral booth (vid. Smartmatic, 2004).

b) the second system, used for instance by *Indra* in Argentina, has also paper trails, but it does not give them to citizens. The machine prints the receipts, it shows them to the voter and finally it

stores them in its own urn. If the voter changes his/her mind before accepting the receipt, he/she may go back to a previous stage and the document will be destroyed.

Anyway, are these different solutions, with or without optical ballots, really enough to guarantee an individual verification of the votes? The answer should be negative. As said before, these systems have only an exceptional use since, in case of a general manual recount, it would have no sense to develop an electronic procedure. Therefore, the voter will not have immediate control over his/her vote and there will not be an individual verification system similar to the current one.

The partial recounts could be the solution. There will not be a general traditional tally, but the organizers would choose a random representative selection of urns in order to check, only in these polling stations, the concordance between the electronic and the manual results. If these verifications are correct, we could maybe reasonably assume that, even without a universal recount, the machines had no errors.

Venezuela, for instance, used this system during the last national referendum in 2004. The elections were very problematic because there was not enough confidence in the transparency and honesty of the electoral board. Once performed the electronic tally, some political groups disagreed with the mechanism and said that the elections had been tampered. The organizers decided then, jointly with the observers of the Carter Center and the Organization of American States, to carry out a second recount in a traditional format, but only with some urns. Since the results of this second tally were the same of the first one, most people accepted them, but it would be useful to make a deeper analysis in order to obtain some suggestions either for Venezuela or for future elections in other countries.

Once accepted this second recount with paper receipts, one of its critical aspects is the mechanism to choose a really random selection of urns. Venezuela used a software developed by the electoral board itself and the Carter Center said that its observers could check it previously (The Carter Center, 2004: [3]). However, Ricardo HAUSMANN and Roberto RIGOBÓN, analyzing the data offered by the opposition groups, said that the electoral board did not allow to use a software of the Carter Center (2004: 21) and that the random selection was finally non-representative: «la muestra utilizada para la auditoría realizada el 18 de agosto no fue aleatoria ni representativa del universo de centros ... [ya que] fue escogida aleatoriamente pero solo entre aquellos centros cuyos resultados no habrían sido alterados» (the sample used for the audit carried out the 18<sup>th</sup> August was not really random nor representative of the polling stations ... [because] it has been chosen only within those stations where the votes had not been tampered) (2004: 2).

This document has the inherent limitations of a statistical study, but it is important to underline that a partial random recount may be useless for a verification procedure if there are not enough guarantees. It is necessary to foresee independent audits and, among other obvious conditions, the paper receipts should have a permanent supervision and the random selection should be carry out by neutral agents and not by the electoral organizers themselves. The audit of the software may be a good solution, but, taking into account the difficulty to achieve a good supervision of these elements, it would be better, as proposed in Venezuela, to use an independent software, that is, a software not controlled by the electoral board.

Obviously, there can be another option of paper trails if the citizen leaves the polling station with a receipt, but the electoral rules use to allow only documents with partial information (vid. Council of Europe, 2004: § 51-52; Mitrou, 2002: 19). It would be feasible therefore to check that one citizen has cast his/her vote –participation receipt—, but not the content of this vote –voting receipt—. This requirement intends to reduce the cases of coercion and/or votes sales that, as Andreu RIERA says, could be massive with electronic tools. The network would allow massive exchanges of voting receipts without the current logistic barriers, that is, the necessity of a person-to-person strategy to buy votes (Fundació Jaume Bofill, 2000: 35-36).

Anyway, these solutions are only feasible within polling stations and we should wonder if similar options are included in remote e-voting systems from other places, either with computers or with phones. At least nowadays, these e-voting procedures do not give nor store voting receipts in a secure form.

With the technology that currently exists, the best guarantee would be giving to the citizen a receipt with an alphanumeric code that would not include the content of the vote. The CETIB's internal regulation includes this solution for the renewal of its Board and, among other examples, *ScytI* used it in the citizen consultation MadridParticipa (Barrat / Reniu, 2004). The administrators publishes at the end of the electoral day the list of processed codes and the citizen could check it and verify that his/her code is in this list (vid. Barrat / Reniu, 2004 and 2004a). It is a good measure because it could strengthen the citizen confidence in e-voting technologies, but it is also true that these options are not enough because, without other complementary solutions, the danger of tampered elections in an invisible way for citizens is still significant. The system is very difficult to understand for an average citizen and there is no clear evidence that the published codes have been actually those used by the electoral board for the tally.

The receipt does not guarantee as well that the vote is finally included in the tally. At least with the system developed by *ScytI* (Riera, 2005: slide 7), the receipt guarantees that the electoral board receives the vote, but there is no control over further stages, that is, the mixing of the votes and the tally. The composition and faculties of the electoral board remain then the only guarantees in this final process. On the other hand, *Indra*, the company managing the electoral process in the schools, does not foresee a method with similar receipts and therefore a voter has no chance to check that his/her vote has been really taken into account.

Actually both cases –CETIB and Andalucia— could admit an at least partial traditional second tally. Despite the existence of a non-presential electronic voting, there is also another option that allows to vote in an official polling station. They are therefore two channels and the suffrages cast by this second one could receive a different treatment and, increasing the guarantees of the overall process, include paper receipts and admit finally a traditional tally. There will be, of course, technical obstacles, like the necessary division of both e-voting channels, but it seems a feasible measure. While CETIB's election foresees as a compulsory measure the option to vote by electronic means in a controlled polling station (art. 40 § 4), the school's bill includes this solution only as an optional one (art. 2 § 2 / Anexo III). Anyway, even the first one has not real paper trails because it only offers the same alphanumeric receipt just described.

Once analyzed these different types of paper trails, we can conclude that there is no way to include in e-voting systems an individual verification of each vote similar to the current one. The random tallies, maybe the closest solution, are not individual verification methods because, although including manual recounts, they intend to guarantee the total tally and not the correct management of a single vote. Those polling stations not chosen in the random selection will have no chance to make an individual verification of each vote. Therefore the reliability of e-voting systems depends only on universal verification methods and we have forgotten the double guarantee, individual and universal, which the traditional electoral system offers with a very simple scheme.

If this is the current situation, we should wonder if the democratic principles are actually compatible with an electoral procedure where there are only universal guarantees. This is one of the main obstacles for the implementation of e-voting solutions because we realize that the citizen loses the supervision power that he/she owns today and the computer experts and the electoral administration itself strengthen their power. The citizen will not be able to be confident into the system itself and he/she will depend on third parties like the two actors just mentioned. A consolidated democracy, where the electoral administration has great credibility among the citizenry, could maybe admit this

situation, but this solution is much more difficult to accept in countries where there are great suspicions about the electoral transparency. The individual verification may play here an important peacekeeping role and it should not be suppressed.

Anyway, it will be useful to analyze if a universal verification system could compensate the absence of a complementary individual control. The best guarantee in this field is a complete audit of the software or, using the terms of the Council of Europe's Recommendation, «the components of the e-voting system» (Council of Europe, 2004: § 24).

### 3.2. Source code.

These elements can only be analyzed by computer experts, but, if there are enough flexible mechanisms, the suspicions of corruption could be eliminated. The best option would be obviously to have a source code completely open to any person, but, as an alternative measure, certain experiences give it only to the electoral authorities and/or other actors like the leaders of the political parties. Therefore, an average citizen, even those with computer skills, will not be able to receive this information. The Council of Europe's Recommendation accepts a partial disclosure of these elements giving them only to the electoral authorities (Rec. § 24-25), but we wonder if these measures are enough from a democratic point of view.

Actually these obstacles could be contradictory with what we say before about the role of the electoral boards in some problematic countries and the usefulness of the current individual verification to overcome these difficulties. A good universal verification became the best solution to compensate the absence of the other type of verification and to avoid a blind confidence of the citizen into electoral administrators maybe not enough transparent and reliable, but to reduce the disclosure of the computer components damages the chances of the universal verification to substitute, or at least to approach to, the role that nowadays plays the individual verification.

If the source code and other critical data are only available to the electoral administrators and the political parties, the citizenry has no way to compensate the loss of power generated by the disappearance of the individual verification. If we broaden the number of people who receive this information, even if we decide to make a full disclosure of the code, a voter will have more confidence because, besides the control of the electoral administration, any citizen with enough computer skills will be able to analyze the code and reveal its errors. To reduce the transparency is always a worrying path and we should try to change this tendency achieving the broadest possible disclosure of the e-voting components. Actually there are some countries that follow these guidelines. Geneva's government, for instance, is the owner of its voting software and «son code-source est disponible à la consultation (sic) pour les citoyens de Genève» (its source code can be analyzed by the citizens of Geneva) (Hensler, 2004: slide. 7).

On the other hand, the generic terms of the Council of Europe's Recommendation hide a great disagreement between those who backed the necessary control over the whole system, including of course the source code, and those who wanted to limit these audits to its critical elements (Braun, 2004: 51). Anyway, either the first or the second solution are in the correct path to achieve reliable systems capable to compensate the disappearance of an individual verification similar to the current ones.

Our four cases offer different solutions. The school electoral process, for instance, has a control body «formado por un grupo de expertos de la Universidad y la Administración» (whose members are experts from the University and the Government) (art. 3 ORD). Its members are nominated by the government and the elected people are included in the same legal decision that we are analyzing. There are seven experts, four from the regional administration itself –parliament and government— and three from the University (two lawyers and one computer researcher). Although none of them

comes from the educational branch of the government, managing institution of the elections, it would be advisable to have more independent actors than people related to the administration in this important body for the security of the e-voting procedures. The nomination should also include some participation of the schools.

The legal resolution has a general mention to the functions of this Committee (art. 3) and there is also another more specific article that could allow any decision, even the compulsory disclosure of the source code for its audit (art. 13). It would be better however to detail more these hypotheses even with specific deadlines for the competent bodies and making compulsory the publication of a specific report. There is no information as well about the binding or non-binding effects of the decisions of this Committee.

The other two examples do not foresee a similar body, but their reasons are probably different. The Basque systems, based on optical ballots, do not need complementary control measures because the paper ballots will not be destroyed and they are the most efficient audit method. However, as mentioned before, these documents do not include a traditional tally and they prefer the so-called electronic-manual one. On the other hand, the Engineering Association's e-voting system is very similar to the school's one, but there is no any general supervision body.

### 3.3. Electoral board.

Any traditional voting process has a specific administration that guarantees the democratic requirements of the elections and one of the most frequent methods is to empower certain citizens with these faculties. In Spain, for instance, a lot of citizens are members of the polling station's boards during the electoral day and they must guarantee the voters' rights. Therefore an independent and neutral structure assumes the responsibility of the electoral organization. The Basque case reproduces this scheme without innovations because its system of optical ballots does not alter the electoral bodies.

The others have a different framework since any remote e-voting system needs to adapt certain traditional electoral patterns. Aiming to reduce the technicians power, both of them foresee specific electoral boards composed by third parties not involved in the electoral organization —citizens, independent experts, observers, etc.—. These committees guards the private key necessary to open the counting server (vid. Barrat / Reniu, 2004a). Each member has a part of this key protected by a password and it will be necessary to join a minimum number of them to rebuild the key, open the urn and make the tally. It is a good measure, but it is not enough because the electoral board should have full access to the computer components, including the source code, in order to check that at least the counting server actually has the mentioned cryptographic protection. Therefore, the importance of this measure depends on the solution provided in the previous section to the audit of the software components.

On the other hand, although both cases agree in create these boards, there are significant differences and it would be useful to analyze each regulation. The Engineering Association, for instance, rules with detail who will be the members of this Committee including either representatives of the current Board —its Secretary— or other members depending on their ages or their affiliation data (art. 39). Finally, there will also be representatives of the different candidatures. It is therefore a large and plural committee and its critical functions will not be controlled neither by the current members of the Board nor by certain parties that, like the candidates, could be interested in.

The *Orden* of the parents' boards does not offer a detailed solution for this item because each school should nominate afterwards the members of their own committees (art. 2.1 *in fine* / Anexo III / Orden). It is a good option because there will not be a centralized structure, one of the main risks of these procedures, but each center should carry out a nomination with neutrality and plurality. Since the

*Orden* does not give more details, there are no guidelines for each school and they will be the maximum responsables.

Finally, their faculties are not the same and there are two important issues to be underlined. While the electoral board of the Engineering Association must “precintar i custodiar l’ordinador urna, l’ordinador control i l’ordenador escrutini” (precint and guard the computer that stores the votes and the control and counting servers) [art. 39 § 3 d)] and, at the end of the electoral day, it will also “desprecintar i ordenar executar l’escrutini electrònic” (deprecint the server and decide the beginning of the electronic tally) [art. 39 § 3 e)], the school’s *Orden* only mentions the protection of the cryptographic keys, but not the same function for the computer servers. Without this measure, it would be feasible to carry out a remote tally and the counting computer, which will not be isolated, could not be at the same place of the electoral board. This is not a problem from a technical point of view, but the citizen confidence would increase if this component is placed during the electoral period in a specific and isolated area controlled by the members of the electoral board.

There is as well another important difference relating the protection of the keys since the CETIB’s regulations foresee a specific security system. The electoral board, for instance, would have a copy of the logins and passwords of each voter in order to give them a copy in case of necessity (art. 40 § 9). This is only an identification measure, but there are also other similar procedures for the auditability. Although not very clearly, another article seems to enlarge the board’s functions with a security copy of the cryptographic keys of the counting server: “Les funcions de la Mesa Electoral són ... d) Precintat i custodiar l’ordinador urna, l’ordinador control i l’ordinador escrutini *i custodiar els duplicats dels identificadors i claus d’accés*, així com la identificació dels col·legiats i la seva inclusió al cens electoral definitiu abans de fer a mans el duplicat de l’identificador i clau d’accés que els hi demanin” (The functions of the Electoral Board are ... d) To precint and guard the computer that stores the votes and the control and counting servers *and to guard the copies of the identifiers and the passwords*, as well as the members’ identification and their inclusion in the definitive roll before giving them the identifier and the password requested) [art. 39 § 3 d); the italic is mine].

This measure intends to reduce the dangers of any centralized procedure, but it creates another risk because the board will have critical information and it will be able to tamper the elections. The remote voting in parents’ school Boards does not include these controls of the cryptographic keys.

Finally, as mentioned, the existence of this sort of electoral boards shows us that a high-centralized structure either of people and machines is an important risk for remote e-voting procedures. In certain cases, for instance, the data of any polling station go to a central computer where the tally will be carried out (Fundació Jaume Bofill, 2000: 17). Any incident, like the impossible meeting of a minimum number of the cryptographic key owners or if they forgot the passwords, may avoid the process and therefore there will be no final tally. The traditional system allows, on the other hand, to isolate those errors. As Jordi CAPO says, the current electoral structure is not dangerous because it has a decentralized scheme and, if there is any exceptional incident, the total process would not be damaged (Fundació Jaume Bofill, 2000: 14).

This is therefore a serious weakness of those e-voting systems. There would be a solution by having a trusted third party that will save the keys and the passwords, but this measure solves only the danger to forget the logins and passwords, but not the centralization risk. On the other hand, a decentralized procedure, similar to the current traditional tally, could be implemented. Despite the economic, technical and logistic risks that have to be analyzed, different e-voting electoral boards could have cryptographic keys and passwords to be used only in case of collapse of the central board.

The parents’ election, maybe for its own nature, foresees this sort of tally because each school will have an electoral board (art. 2.1 / Anexo III / ORD). Therefore the possible collapse of nine schools has been foreseen. There is still the same risk within each center, but this degree of centralization

would be more or less the same that we find nowadays. Alternative boards and tallies would reduce even more this problem and it should be analyzed from a technical point of view.

#### 4. CONCLUDING REMARKS.

The four legal documents that have been analyzed show a common effort to include auditability mechanisms, but each one prefers different measures. There are, for instance, paper trails, supervisory independent bodies or plural electoral boards. However, it would be better to strengthen even more these control measures because there are some weak elements that have to be reconsidered.

Optical ballots have a very easy way to create citizen confidence, but the Basque solution does not include a manual tally and it prefers to use the ultraviolet reader. While this is not a bad measure, it would be interesting to analyze a possible traditional count with only the paper ballots used by citizens to cast their votes. On the other hand, the existence of a supervisory body is very useful for any e-voting system, but legal documents should detail, among other things, whether its decisions are binding. Finally, the cryptographic keys are a critical component of some e-voting methods and therefore any legal ambiguity about its use, like a non-clear regulation about the security copies, should be avoided.

Anyway, the translation of technical conditions into specific legislations requires a long path that, at least in Spain, is just beginning. International guidelines and national documents should take into account the different e-voting systems and include detailed legal patterns that could generate enough citizen confidence in these new technologies.

#### 5. REFERENCES.

- Ambrosio i Gomàriz A. d' 1999. *Iniciació al vot electrònic*, (Col. "Quaderns Electorals – 3"), Barcelona: Generalitat de Catalunya / Departament de Governació.
- Arnaldo Alcubilla E and Ambrosio A. d'. 1998. 'El voto electrónico: algunas experiencias recientes'. *Cuadernos de Derecho Público*, 4: 159-175.
- Barrat i Esteve J and Reniu i Vilamala J. M.  
2004. *Informe de las experiencias de voto electrónico empleadas en las elecciones catalanas de noviembre 2003*, León / Barcelona: Universidad de León – OVE / Universitat de Barcelona.  
[www3.unileon.es/dp/aco/area/jordi/treballs/evot/cat03.pdf](http://www3.unileon.es/dp/aco/area/jordi/treballs/evot/cat03.pdf)
- 2004a. *Electronic Democracy and Citizen Participation. A Sociological and Legal Report about the Citizen Consultation "MadridParticipa"*, Madrid: Ayuntamiento de Madrid.  
[www3.unileon.es/dp/aco/area/jordi/treballs/evot/lilibreang.pdf](http://www3.unileon.es/dp/aco/area/jordi/treballs/evot/lilibreang.pdf)
- Braun N. 2004. 'E-Voting: Switzerland's Projects and their Legal Framework – in a European Context' in PROSSER, Alexander / KRIMMER, Robert (eds.) *Electronic Voting in Europe. Technology, Law, Politics and Society*, (Col. "Lecture Notes in Informatics (LNI) / P-47"), Bonn: Gesellschaft für Informatik, pp. 43-52.
- Cetib  
2004. *Proposta de modificació dels Estatuts del Col·legi d'Enginyers Tècnics de Barcelona*, Barcelona: Col·legi d'Enginyers Tècnics de Barcelona – CETIB.  
[www.cetib.net/cat/public/informacio/documents/edem-proposta.pdf](http://www.cetib.net/cat/public/informacio/documents/edem-proposta.pdf) [2<sup>nd</sup> March 2005]

- 2004a. 'La Junta General aprueba la modificación de los estatutos y los presupuestos de 2005'. *Informatiu Theknos*, 85, Reportaje, Barcelona: Col·legi d'Enginyers Tècnics de Barcelona – CETIB.  
[www.cetib.net/cat/public/informacio/versio-esp/reportatge0501.pdf](http://www.cetib.net/cat/public/informacio/versio-esp/reportatge0501.pdf) [2<sup>nd</sup> March 2005]
- Boja. 2005. Orden de 29 de diciembre de 2004, por la que se regula la aplicación del voto electrónico en los procesos electorales para la renovación y constitución de los Consejos Escolares 2004-2005 en los centros docentes que se relacionan, *Boletín Oficial de la Junta de Andalucía*, 11, 18<sup>th</sup> January 2005, pp. 6-9.
- Council of Europe. 2004. *Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical standards for e-enabled voting (IP1-S-EE), Integrated Project 1 – Making Democratic Institutions Work, IP1 (2004).  
[www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2Dvoting/02\\_Recommendation/Rec\(2004\)11E\\_rec\\_adopted.asp#TopOfPage](http://www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2Dvoting/02_Recommendation/Rec(2004)11E_rec_adopted.asp#TopOfPage) [2<sup>nd</sup> November 2004]
- Eusko Legebiltzarra. 2004. *Proyecto de Ley de reforma de la Ley de Elecciones al Parlamento Vasco*, Vitoria: Eusko Legebiltzarra.  
[parlamento.euskadi.net/pdfdocs/publi/1/07/000156.pdf#19614](http://parlamento.euskadi.net/pdfdocs/publi/1/07/000156.pdf#19614) [2<sup>nd</sup> March 2005]
- Fernández Riveira R. 2001. 'El voto electrónico: el caso vasco'. *Revista de Estudios Políticos*, 112: 199-236.
- Fundació Jaume Bofill. 2000. *La votació electrònica: un debat necessari*, (Col. "Debats de l'Aula Provença – 33"), Barcelona: Fundació Jaume Bofill.
- Gritzalis D. A. (ed.). 2003. *Secure Electronic Voting. Advances in Information Security*, Boston: Kluwer.
- Hausmann R and Rigobon R. 2004. *En busca del cisne negro: Análisis de la evidencia estadística sobre fraude electoral en Venezuela*, Harvard University / Massachusetts Institute of Technology.  
[www.proveo.org/hausmann.pdf](http://www.proveo.org/hausmann.pdf) [9<sup>th</sup> September 2004]
- Mitrou L *et al.* 2002. *Legal and regulatory issues on e-voting and data protection in Europe*, E-Vote Project.  
[www.instore.gr/evote/evote\\_end/htm/3public/doc3/public/public\\_deliverables/d\\_3\\_4/e\\_vote\\_D\\_3\\_4\\_v22\\_20\\_02\\_02.doc](http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/public_deliverables/d_3_4/e_vote_D_3_4_v22_20_02_02.doc) [10<sup>th</sup> January 2004]
- Riera A. 2005. 'Què es necessita per que [sic] el vot electrònic remot sigui segur?'. *II Jornades de Signatura Electrònica*, Agència Catalana de Certificació /CatCert.  
[www.js-e.net/cat/Archivos/ponencies\\_web/Andreu\\_Riera.pdf](http://www.js-e.net/cat/Archivos/ponencies_web/Andreu_Riera.pdf) [21<sup>st</sup> July 2005]
- The Carter Center. 2004. *Last Phase of the Venezuelan Recall Referendum: Carter Center Report*, The Carter Center, 21<sup>st</sup> August 2004.  
[www.cartercenter.org/doc1807.htm](http://www.cartercenter.org/doc1807.htm) [23<sup>rd</sup> August 2004]
- Trechsel A. H and Mendez F (eds.). 2005. *The European Union and E-voting. Addressing the European Parliament's internet voting challenge*, London: Routledge.