E-COGNISING: THE E-VOTING TOOL FOR E-COGNOCRACY*

MORENO-JIMÉNEZ , José María[(1)+]
PILES, Joan [(2)]
RUIZ MÁS, José [(2)]
SALAZAR, José Luis [(2)]

(1) Grupo Decisión Multicriterio Zaragoza
(2) Grupo Tecnología de la Comunicación
Universidad de Zaragoza. Spain

ABSTRACT:

E-cognocracy (Moreno-Jiménez, 2003a, 2006; Moreno-Jiménez and Polasek, 2003, 2005) is a new, creative, innovative and cognitive democratic system that, based on the evolution of living systems, focuses on the extraction and social diffusion of the knowledge derived from the scientific resolution of high complexity problems associated with public decision making related with the governance of society. Using multicriteria decision making and data mining techniques as the methodological aid, the democratic system as a catalyst for the learning that guides the cognitive process that is distinctive of human beings and the Internet as a communication support, e-cognocracy resolves some of the limitations of traditional democracy and provides room for greater involvement of the citizenry in their own government. To that end, we present a new technical tool, *e-cognising*, which allows for a secure e-implication of citizens in the resolution of public decision making problems, to joint the set of OR methodologies and tools employed in the DSS we are developing for this cognitive democracy.

KEYWORDS: egov-DSS, e-democracy, e-voting, e-cognocracy, e-cognising, multicriteria, internet, knowledge, security.

INDEX:

* An earlier version of this paper was presented at the EWG on DSS held at London, 2006. The work has been partially funded under Research Projects "*E-participation, Security and Knowledge Democratisation*" (Ref. PM2007/034) and "*Internet-based Complex Decision Making. Decisional Tools for e-cognocracy*" (Ref. TSI2005-02511).

[+] Corresponding author (moreno@unizar.es).

1.INTRODUCTION

During the last 25 years we have witnessed the continuous appearance of decision support systems (DSS) in almost all fields of human activity, in particular in those related with the private domain, that is to say, with entrepreneurial decision making in the business world (Eom et al., 1998; Eom and Kim, 2006; Arnott and Pervan, 2005). By contrast, one of the fields with a lower incidence of these kinds of tools is the public domain, more specifically, public decision making related with the governance of society (egov-DSS). Fortunately, many institutions, starting with government itself (e.g. the EU's Sixth Framework Programme), have become conscious of this lacuna (egov-DSS), seeking the solution of this problem, and a greater involvement of the citizenry in their own governance, by various means.

Focusing on the specific case of democracy and due, among other things, to the lack of participation and transparency of democratic systems, a dangerous idea has arisen that the political class lack legitimacy. This, in turn, has led people to speak of the *fallacy of democracy*, in that this form of representation no longer meets its initial objectives, namely the participation of citizens in their own government.

With the aim of recovering the credibility of the democratic system that governs western societies, many voices have been raised which, taking into account the development of the information and communication technologies (ICTs), as well as the OR methodologies and tools in this field (see http://infodoc.escet.urjc.es/ted/), advocate the development of DSSs which favour the direct participation of citizens in the governance of society and their assistance in public decision making (egov-DSS).

Unfortunately, at least at the present time, when the political class talk about encouraging transparency and participation, they do so exclusively from their own point of view. In order to deal with both questions, they propose to provide more information to the citizens about the way they are operating (transparency) and to seek from them their opinions about the most interesting topics or problems, as well as their suggestions about the way to achieve their resolution (participation). At the end of the day, it is precisely the elected representatives who continue to take the decisions, in many cases thinking only of the interests of their respective political parties, and not those of the citizen or the society as a whole.

In order to overcome these limitations of traditional democracy, and to enable the greater involvement of the citizenry in their own government, a new and creative democratic system called *e-cognocracy* (Moreno-Jiménez, 2003a, 2006; Moreno-Jiménez and Polasek, 2003) has recently been proposed, one that is based on the evolution of living systems.

Combining representative and participative democracy, e-cognocracy focuses on the extraction and social diffusion of the knowledge derived from the scientific resolution of high complexity problems associated with public decision making related with the governance of society. This innovative proposal effectively eliminates the weakness suffered by both democratic systems (representative and participative) when each of these is considered in isolation, and facilitates a true electronic implication (*e-implication*) of citizens in the decision making process, rather than just the constrained *e-participation* in the debate and discussion of problems (e-democracy).

E-cognocracy, also known as cognitive democracy, uses the democratic system as a catalyst for the learning that guides the cognitive process distinctive of human beings, the multicriteria decision making and data mining techniques as the methodological aid

and the Internet as a communication support. The combination of these three scientific fields: Political Theory (democracy), Decision Theory (operations research tools) and Information and Communication Technology (collaborative and communicative tools) establish the conceptual framework necessary for designing the DSS used to deal with "new" public decision making related with the governance of society (egov-DSS).

In order to take up this challenge, this paper is centred on the development of a new communication and discussion tool (*e-cognising*) which, in a technologically secure way, allows us to address the e-implication of citizens in solving public decision making problems, meeting the generic properties of the classical e-voting systems and the specific properties associated with this cognitive democracy (Moreno-Jiménez, et al., 2006b; Piles et al. 2006a,b; Salazar et al., 2008).

To that end, the paper is structured as follows. Section 1 establishes the framework of our proposal. The concept of e-cognocracy, its justification from the point of view of the evolution of living systems and its differences with e-democracy are considered in Section 2. Section 3 describes the steps of the procedural methodology of e-cognocracy and summarizes some decisional tools developed for the practical application of cognitive democracy. Section 4 analyses the technical security properties from the point of view of the traditional e-voting systems, before turning to the specific security needs required for e-cognocracy and presents the structure of egov-DSSs. Section 5 presents e-cognising, the new e-implication system developed for e-cognocracy and offers a technical solution to address the new needs of *linkability* and *anonymous weighting*. Finally, Section 6 closes the paper with a review of the main conclusions and future lines of research.

2. E-COGNOCRACY

E-cognocracy (Moreno-Jiménez, 2003a, 2006; Moreno-Jiménez and Polasek, 2003, 2005) is a new democratic model that tries to make more ambitious use of democracy than the mere election of political representatives. In this regard, based on the evolution of living systems (only species that learn –extract and spread knowledge– and which adapt to the context, are able to survive), e-cognocracy focuses on the extraction and social diffusion of the knowledge derived from the scientific resolution of high complexity problems associated with public decision making related with the governance of society.

If the representative process of traditional democracy corresponds to the security and social needs of the second and third level of Maslow's Needs Hierarchy (Maslow, 1943), respectively, then, for its part, the cognitive process of e-cognocracy focuses from a social point of view on the first and more basic level of this hierarchy, the *physiologic needs* (learning for survival). Having said that, it could also be considered at the top level of the hierarchy (self-actualisation), if the individual cognitive process is taken into account.

The cognitive approach adopted in our proposal tries to use democracy to met basic needs. This orientation reflects in a way, what happens in the evolution of living systems, where *genetic diversity* and *natural selection* take the form of *knowledge diversity* (plurality of opinions) and *personal selection* via the Internet.

Following the guiding vision of e-cognocracy, that is to say, there is no democracy without freedom and there is no freedom without knowledge (Moreno-Jiménez, 2003a), its main aim is to pursue the democratisation of knowledge as the way to improve the quality of live of citizens, an objective that is achieved by means of the creation of a

new, more open, transparent, civilized and free society, which is, at the same time, more cohesive and connected, and more participative, equal and caring.

To that end, e-cognocracy combines the two most extended democratic models, representative democracy (the new right) and participative democracy (the new left), in a cognitive democracy, where decisions are made by combining the results obtained from the political parties (representative democracy) and citizens (participative democracy). To aggregate these results (see Figure 1), we use different weights (w_1 and w_2) depending of the context of the problem (local, regional, national or supranational) and the objectives of the system.

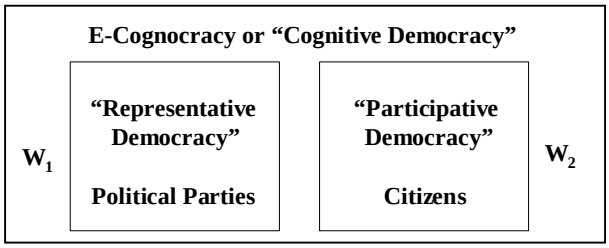

Figure 1: E-cognocracy

The combination of these two democratic models with appropriate weights allows us to overcome most of the limitations of both systems. With respect to representative or legal democracy, where elected "functionaries" assume the representation of the citizens' interests in a legal framework, these limitations are (Moreno-Jiménez and Polasek, 2003): specific participation confined to the election of representatives; control of electoral list by the political parties; hiding of critical positions and interest, as well as a clumsy system with slow participation. As regards participative or direct democracy, where the citizens are directly implicated in the decision making process, the limitations are (Moreno-Jiménez, 2006): populism and the lack of a global perspective of problems.

The key characteristics of the e-cognocracy are:

(a) Human beings are considered in a holistic and systemic context.

(b) Citizens may participate in the system either as they have traditionally done (delegation), or by taking part directly in the resolution of problems. It allows for direct involvement of the citizen in decision making processes, thereby fostering participation in the democratic system and the creation of knowledge in society.

(c) Parliament would be distributed in two parts (public and private). The share of seats allocated to each part is around (2/3 and 1/3).

(d) In order to avoid saturating citizens with participation in these processes, only some particularly relevant problems (strategic problems) would be treated in this manner.

(e) In order to solve the problem, including the aggregation of the solutions provided by political parties, on the one hand, and citizens on the other, we use multicriteria techniques.

(f) Using this model, we are able to extract knowledge as this refers to behaviour patterns, preference structures, stylised facts and trends of the decision making process.

(g) Internet is used to incorporate the preference structures of citizens into the decision making process.

(h) It improves control of the political system and reduces dependence on minority political groups, since it would be essential to win a margin of (online) votes for each problem and at any given moment. This would produce wider coalitions between groups, favouring more moderate proposals enjoying democratic support.

(i) All ideas, even minorities' positions, are included, but decisions are taken according to the majority rule.

(j) It improves overall knowledge and understanding of the system, incorporating a wider range of perceptions of reality, deepening debate and strengthening negotiating processes and the search for consensus.

(k) Effort, learning and continuous improvement are favoured, and recognition should be given to the skills and abilities of individuals, thereby identifying social leaders.

(l) It facilitates continuous education (learning) of the interested population, in line with the Rawlsian concept of social justice (i.e. equality of social opportunities).

(m) It allows for easy expansion and diffusion of knowledge (socialisation of knowledge), as well as the creation of minimum ethical standards. In this way, ignorance, which is the real poverty suffered by humans beings, can be reduced.

Summarising, the key idea of e-cognocracy is to educate people (intelligence and learning), promote relationship with others (communication and coexistence), improve society (quality of life and cohesion) and construct the future (evolution) in a world of increasing complexity (Moreno-Jiménez, 2006).

3. OR-METHODOLOGIES AND TOOLS FOR E-COGNOCRACY

If traditional democracy was characterised by the idea of "one person one vote" and the filtering of political decisions by the political parties, e-cognocracy is defined by the idea of "one man many ideas" and that fact that these are filtered by the citizens themselves through open and public choices made on the network.

E-cognocracy seeks to convince citizens of the appropriateness of a given decision constructed online by all concerned. It does not seek, as has so often been the case with representative and participative democracy, to defeat or dominate adversaries by winning a majority of parliamentary seats, only for subsequent decisions to be taken that are frequently unrelated with the parties' initial electoral programmes.

If e-democracy refers to the participation via the internet (e-participation) of citizens in public decision making, where this participation, in practice, consists of citizens simply offering their comments, opinions and suggestions to the elected representatives (debate and discussion for assistance), e-cognocracy refers to the implication[1] via internet (e-implication) of citizens in public decision making, that is to say, their direct intervention in the decision making process (decision).

Within this framework, we must develop OR methodologies and tools to deal with the design of egov-DSSs that assist in the scientific resolution of highly complex problems corresponding to public decision making related with the governance of society. Following the cognitive approach we propose, the decision making process does not conclude, as is habitually the case, with the selection of the best alternative. Rather, the final and essential step of this process is the creation and diffusion of knowledge, where this knowledge corresponds to the patterns of behaviour of the actors involved in the resolution process. Thus, the main idea is to identify the arguments that support the

[1] When cooking eggs with bacon, the chicken participates and the pig is implicated.

different positions of individuals and political parties, and to offer the citizens these arguments in an easy to understand way that allow them to reach the corresponding learning process.

The methodology employed is based on the cognitive constructivism that characterises the multicriteria procedural paradigm (Moreno-Jiménez et al., 1999; Moreno-Jiménez et al., 2001; Moreno-Jiménez, 2003b) that we have followed to solve highly complex public decision making problems (see http://cmisapp.zaragoza.es/ciudad/presupuestos-participativos/ in a real application for the Zaragoza City Council).

In recent years, the traditional scientific method characterised by objectivity, rationality, causality and seeking for a single and universal truth is being replaced by a new scientific method (Moreno, 2003b) which allows for the consideration of the subjective, the intangible and the emotional, associated with the human factor, in tune with recent social thinking and needs. This new context must be able to integrate the objective of classical science, on the one hand, with the subjective in human behaviour, on the other, into one global end, basically aimed at the creation and social diffusion of knowledge. In essence, the search for truth that characterises the traditional scientific method is gradually being replaced by the search for knowledge[2] as the criterion to guide decision making and the scientific resolution of complex problems from a holistic and systemic point of view.

As the multicriteria framework proposed in our approach to deal with the incorporation of different actors and the integration of the objective with the subjective, as well as the rational with the emotional, we have selected one of the most extended methodologies: the analytic hierarchy process (AHP) of Saaty (Saaty, 1980, 1996). This approach, in common with all the multicriteria schools, suffers from a number of drawbacks. Nevertheless, from our cognitive point of view, an aspect which is more important even than the specific resolution of the problem is the knowledge extracted from the exploitation of the mathematical model. An objective treatment of the subjective guarantees the scientific character of the procedure followed. As Bernard Roy (1993) argues, this character will be given by the rigour, transparency and accessibility of the method applied.

With respect to the specific OR tools that the Zaragoza Multicriteria Decision Making Group has developed for e-cognocracy in the context of AHP, it should be mentioned that these decisional tools correspond to specific questions which arise in the different stages considered in the resolution process of a problem from a practical point of view. The procedural steps considered in e-cognocracy, which obviously are independent of the methodology employed in its application (AHP in our case) are:

Step 1: *Formulation of the problem*. Government, political parties or citizens, when they overlap some specific thresholds, may propose (Moreno-Jiménez, 2006).

Step 2: *Determination of actors involved in the resolution process*. Political, methodological, technical and juridical actors must be established before the resolution of the problem.

Step 3: *Modelization of the problem.* Using any of the existing collaborative and methodological tools, the problem will be modelled through Internet by all the actors involved in the resolution process.

[2] Understood as the interpretation of information in a specific domain.

Step 4. *Preference elicitation*. Once a specific model is determines for the problem in the previous step, individual preferences are incorporated into the system using Internet, after a debate and discussion of different positions.

Step 5. *Selection of the best alternative*. Using any multicriteria approach, the individual and social ranking of alternatives are obtained.

Step 6. *Extraction of patterns of behaviour*. With the help of multivariate techniques and data mining tools, different patterns of behaviours are identified and associated with the arguments that support them.

Step 7. *Diffusion of patterns o behaviours*. Using Internet the patterns of behaviour and the argument that support them (including the intensities given to the different positions) are shared into the network (socialization of knowledge). This way any individual can internalise this information and to improve its knowledge of the scientific resolution of the problem.

Step 8. *New rounds (optional)*. Sometimes is possible to consider new rounds in the resolution process, which seek for an enrichment of it. In this case, it is necessary to develop communication tools that allow us to capture the individual and social learning, and to identify the societal leaders.

Most of our decisional tools refer to Steps 5 (selection of the best alternative) and Step 6 (extraction of patterns). Aguarón and Moreno-Jiménez (2000) define priority stability intervals in AHP. Aguaron et al. (2003) present consistency stability intervals for the geometric consistency index (Aguarón and Moreno-Jiménez, 2003; Escobar et al., 2004). These intervals are used to obtain the core of consistency in AHP-group decision making (Moreno-Jiménez et al, 2005b; Moreno-Jiménez et al., 2006a). From a Bayesian perspective, Altuzarra et al. (2005), Gargallo et al. (2006) and Moreno-Jiménez, Salvador and Turón (2005) provide different tools for pattern identification. Moreno-Jiménez et al., 2005a) summarises some decisional tools for knowledge extraction. Finally, Altuzarra et al. (2006) and Escobar and Moreno-Jiménez (2006) present two procedures to select the best alternative. In the first case, from a Bayesian point of view and in the second, combining AHP with Borda's count methods.

In addition to these OR methodologies and tools, there is a fact that highlights in the practical application of e-cognocracy. This is the e-implication of citizens in the resolution problem. In this regard, it is required to guarantee all the properties needed for a secure electronic intervention of the citizens. These properties and the tool proposed for supporting secure communication and interaction in public decision making are presented in the next sections.

4. TECHNICAL FOUNDATIONS OF E-COGNOCRACY

e-Cognocracy and the e-Voting Process

In e-cognocracy, the decision making process is no longer focused only in the actual choice of the citizens, but also in the way through which this choice has been reached, the actual reasons that interest and move the people (i.e. it is important to know not only the political party chosen, but if it has been chosen because of their economical, social, etc. proposals). This kind of poll is very similar to electoral voting and thus we concentrate on e-voting as the first step towards the gathering of information from citizens. E-cognocracy uses the e-voting process to incorporate the preferences of the decision makers into the decisional process. To this end, it requires new technical tools.

To get the citizens more involved in this process and to extract the relevant knowledge of the decisional process, we have divided each voting into different rounds. Each voter can vote in as many rounds as he or she wants (but only once in each round). After each round, the results are published and are provided as additional information to the citizens. For the results of voting in progress, only the last vote of each citizen is entered. However, all the votes from the same voter are linked together (keeping, of course, the anonymity of the voter). This allows us to track very accurately the shifts in opinion and link them to external events, thus knowing what is really driving people's opinion.

To protect the identity of the voter, the individual trails are not publicized. For example, somebody could be paid to vote first A, then B, then C and, finally, D. Depending on the number of rounds, the number of possible combinations becomes sufficiently great that it is relatively safe to say that each person followed a different chain of votes. However, this chain of votes gives us information that will help to determine the reasons for changes in opinion (e.g., not only that people switched from A to B, but that can be a generalized fact after a specific event). In addition, people are encouraged to put forward their points of view in open forums (anonymously, if that is desired) and the effects of these discussions can be correlated with changes in the opinions of the voters.

Requirements for e-cognocracy

The development of algorithms implementing electronic voting has been wide since its beginnings (Cohen, 1985). The first point to take into account in order to secure an electronic voting is the precise classification of the services to be protected:

• Accuracy

– It shall not be able for a non authorized person to modify any votes (that is, only each voter can cast its vote).

– It shall not be possible to remove a valid vote from the final counting.

– It shall not be possible to include a non-valid vote in the final counting.

• Democracy

– Only voters in the census shall be able to vote.

– Each voter shall be able to vote only once in each round.

• Privacy

– A voter shall not be linked to its vote.

– A voter shall not be able to prove its vote.

• Verifiability

– Voters shall be able to verify that their vote has been correctly accounted.

Most of these services have already been studied, and so including them to e-voting process requires only an adaptation. However, anonymity and the antagonistic duality of verifiability (a voter is given a proof that his vote has been included in the tally) and no coercion (a voter cannot show to anybody a proof of the content of his vote) are specially characteristics of e-voting.

There are three paradigms for the anonymity of cryptographically secure ballot elections:

- Blind signatures (Chaum, 1982). The voters obtain ballots from the authorities, certified and privacy-preserved. This paradigm requires an anonymous channel between the voter and the tallying authorities to hide the user identity at the ballot casting.
- Homomorphic encryption (Cohen, 1985). The ballots are encrypted and classified. This enables these schemes a fast tallying process.
- Mix-net (Chaum, 1981). A recount authority moves and permutes the ballots, while changing their representation.

No coercion and claiming are two optional services and are offered or not depending on the actual scenario of the voting. No coercion means the voter is free from external pressure, be it lucrative (buying of votes) or an extortion (threats). In both cases, the coercive party will require a proof of the vote from the voter. In some e-voting schemas this is possible, as the voter is given a receipt which includes information about the content of the vote. This is intended to provide a tool for the voter to reclaim, should his vote be missing from the tally. This shows how these two services are antagonistic. Providing both services at the same time is possible using vote-tags. On the other hand, providing this service is optional, and will depend on the scenario.

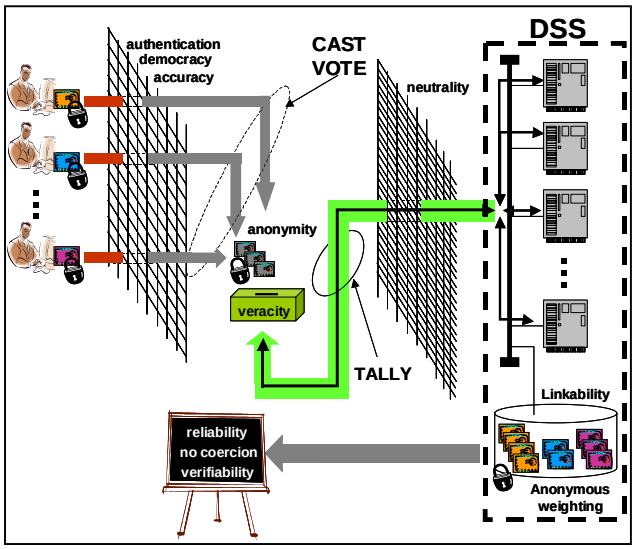

Figure 2: Secure environment for e-gov-DSS in e-cognocracy

E-cognocracy requires the following performance properties (see Figure 2), most of which are shared with the classical systems of e-voting (Benaloh 1994, Cranor 1996):

1. Only voters in the census shall be able to vote (authentication).
2. Each voter shall be able to vote only once in each round (democracy).
3. A voter shall not be linked to its vote (anonymity).
4. A voter shall not be able to prove its vote (no coercion).
5. It shall not be possible to remove a valid vote from the final counting (precision)
6. It shall not be possible to include a non-valid vote in the final counting (reliability)
7. Only each voter can cast its vote (veracity)
8. Voters shall be able to verify that their vote has been correctly accounted (verifiability).

9. For each round the vote should be secret until the recount phase (neutrality).

10. Two votes from the same voter in different rounds of the voting shall be linked together, but not to the voter who cast them (linkability).

11. Allow to one person to sign as a member of a group, but without giving any information about the identity of the signer. (anonymous weighting)

We also must define the parties involved and the roles each one takes, before describing their actuations. These are:

Voter (V): Each voter must show its preferences in a multi-choice question, and rank them numerically. For all rounds of the e-voting, the census shall be constant.

Certification Authority (CA): The Certification Authority shall issue the public/private keys and certificates for each actor involved in the process, and will serve as Trusted Third Party with regard to the validation of certificates.

Recount Authority (RA): The Recount Authority is the only entity allowed to decrypt the votes. The Electoral Authority shall provide information enough to link the votes from the same voter, but not to track them to the actual person who cast them.

Electoral Authority (EA): The Electoral Authority shall keep track of the census, validate the users in the voting process, and sign their votes as a proof of voting. It shall also keep enough data about the votes to know the hash of the last vote from a voter (in order to link them for the Recount server) but without actually being able to decrypt them.

5. E-COGNISING

This section presents e-cognising, the new system developed for e-cognocracy and offers a secure technical solution to address the e-implication of citizens in solving public decision making problems, meeting the generic properties of the classical e-voting systems and the specific properties associated with this cognitive democracy.

To implement the system, we choose the JAVA technology, as much on the client side as on the server side. To minimize the number of configurations in which the client side had to run, we choose a standard web browser, *Mozilla Firefox*. The browser has been completed with some libraries (JSS), needed to be able to access the client certificates which are stored in it from within the JAVA applet that will be the client software. If those libraries were not available, the user should manually add the client certificate and the Certificate Authority to the JAVA application. The application server to use will depend on the available infrastructure at the deployment. In our tests, we are using *Tomcat* as application server. It was chosen to use *MySQL* as a backend to store the data related to the voting.

All of the applications between client and server are encoded and authenticated, using a public key infrastructure implemented through digital certificates and the use of SSL.

Protocol

The implemented voting protocol is the following:

1. The questions are presented to the voter, who then makes his choices. The voter fills the field about his weighting also.

2. Voter identifies himself to EA and sends it a hash of his vote for EA to issue a blind signature of it, and a ticket made from a mix of his identity and a random value that will be signed by EA as well.

3. EA verifies the voter's identity, checking it against the census, that the voter has not already cast its vote in this round and the value of the weighting field.

4. EA issues a blind signature of the vote, and a signature of the ticket, and stores them linked to the voter for future rounds.

5. The voter encrypts his vote and the blinding factor used previously with RA's public key and sends them to EA.

6. EA sends to RA: the vote and the blinding factor, encrypted, the blind signature of the vote and the signed ticket.

7. If the voter had previously voted (in other rounds), EA sends to RA a copy of the blind signature of the latest vote, which will be then used by RA to link them.

8. EA sends to V the signature of the ticket to prove that his vote has been stored.

When the voting time is passed starts the counting time. In this phase we have these steps:

- RA makes public the signatures of the tickets, and starts a claims period before the publication of the results.

- RA decrypts the original votes, and uses the secret included with it to get a valid signature from the blind signature.

- RA checks the vote with the signature obtained and verifies that it is correct.

- RA links all the votes from the same voter.

- RA publishes the results of the round/voting.

Vote linkability and anonymous weighting

As we have said previously, on of the ways through which e-cognocracy tries to get people involved is the identification of the issues that are critical in the decision making process. This is achieved in two ways:

i) Multi-criteria framework: In order to collect the opinion of the people, several key issues are presented to them to vote, still keeping the elected representatives some weight in the choice (e.g. it could be x % direct participation and $(100 - x)$ % indirect participation) in order to stop demagogy.

ii) Linkability of votes: Each poll is divided in several rounds (the number of rounds is fixed beforehand, and each voter can cast each votes in as many rounds as he wants, but only once each round. The last vote cast by each voter (independently of the round in which it was cast) is the one taken into account for the final result. However, all the votes from the same voter are linked together (keeping, of course, the anonymity of the voter). This allows us to track very accurately the shifts in opinion and link them to external events, thus knowing what is really driving people's opinion.

Proof of fitness

Let us see whether our system is adapted to the requirements imposed on e-cognocracy, by examining each one of the properties required:

Authentication. The kind of signature used guarantees that the signer is in the designed group of voters.

Democracy. If one participant cast two opinions in the same round, he should use the same linking-tag and would be detected.

Anonymity. Anonymity is guaranteed by the kind of signature used, and the probability of guessing the actual voter is 1/N, where N is the number of voters in a given group.

No coercion. In exchange for his participation, the participant receives only a signed linking-tag and time-stamp and does not bear a relation to the content of the vote.

Accuracy. Each participant proof to be in a census to the EA, therefore, this one must know the private key, which is impossible to fake, whenever it has a suitable length.

Reliability. Each participant have a signature of the linking-tag that he or she sent to the RA and a list of these linking-tags will be published before the recount; therefore, even if RA is compromised, the participations cannot be deleted, since this action will be reported by the affected participants who will present their signed linking-tags to support their objection.

Veracity. A participation cannot be sent to RA (even if RA is compromised), because it would be necessary to obtain a valid signature, and that is not possible without the private key of the participant.

Verifiability. For each vote received, the RA gives back to the participant a signed inking-tag. Later, when beginning the recount, RA publishes a list of the linking-tags of he participation. If a participant has a participation that is not included in the list, he could report it to the RA so that it undertakes the appropriate action.

Neutrality. RA decrypts the votes once each round is finished.

Linkability. Along with each vote, the EA sends to RA the blind signature of the last vote cast by the same person. In the recount phase, RA searches among the cast votes, one whose blind signature matches it. In that way, a chain of votes is obtained that stores all of the history of the voter without revealing his identity.

Anonymous weighting. Each vote contains a field with the voter weight. That field will be the same in every round and it cannot be changed in the same way that the vote. In the counting phase RA will use it when it will decrypt the linking votes.

6. CONCLUSIONS

This paper presents a technical tool, e-cognising, that allows secure e-implications of citizens in public decision making related with the governance of society. This technical tool is being integrated with other decisional tools that the Zaragoza Multicriteria Decision Making Group has developed during the last years in the context of the analytic hierarchy process (AHP) to design an egov-DSS that can affront the resolution of high complex problems corresponding to public decisions related with the governance of society in an effective and realistic way.

The e-implication of citizens in the resolution of public problems is achieved by using a creative (Simon, 1977) and innovative (McElroy, 2003) public decision making framework, named e-cognocracy. This new democratic model combines the representative and the participative democracy to improve the transparency of the system and the control and participation of citizens. Despite these operative goals are of enormous importance, as the European Community has pointed at the Sixth Framework Programme, e-cognocracy seeks for more ambitious goals than traditional democracy. It pursues strategic goals related with the evolution of living systems.

The essential contribution of this cognitive democracy is the social democratization of knowledge, as a vehicle to favor the survival of human beings. E-cognocracy can be employed to create a new, more open, transparent, civilized and free society, that is at

the same time more cohesive and connected, and more participative, equal and caring. If e-democracy represents the governance of people using ICT, e-cognocracy represents the governance of knowledge and wisdom using ICT.

In order to successfully achieve these goals, OR methodologies and tools have been employed and a new technical support for secure e-implication has been developed. This technological tool (e-cognising) guarantees that the process of discussion and decision making carried out through Internet satisfies the generic properties demanded for traditional e-voting systems, together with those specific properties of linkabilility and anonymous weighting imposed by the particular characteristics of e-cognocracy. Thus, this tool allows one person to sign as a member of a group, but without giving any information about the identity of the signatory and with no previous set up. Furthermore, all the signatures from the same signatory can be linked together, but maintaining anonymity. Additionally, we provide a mean to mark the voters as belonging to different groups, which is useful for e-cognocracy, because, as we said earlier, there can be a mix of direct and indirect participation.

As regards future work, our objective is to improve our proposal by simplifying the process. To that end, our aim will be to eliminate the need for an Electoral Authority without losing any of the services provided and, in addition, to reduce the computational complexity of the linking votes and of the receipt generation. Furthermore, if the vote is sent directly from the voter to the recount authority, we shall give the voter more confidence in the process.

Finally, it is important to highlight the fact that egov-DSSs (i.e. interactive DSSs that assist in public decision making related with the governance of society) present an additional complexity to traditional DSSs, the security of the channels used to incorporate opinions, suggestions and preferences. Secure e-implication is needed to reach the atmosphere of trust necessary to democratising knowledge. In this regard, we present a new tool (e-cognising) for supporting secure communication and interaction in public decision making, which addresses these needs and provides a further step in the evolution of public DSS that is in accordance with recent proposal on Group Communication and Decision Support.

References:

AGUARÓN, J.; ESCOBAR, M.T.; MORENO-JIMENEZ, J.M. (2003): Consistency Stability Intervals for a Judgement in AHP-Decision Support Systems. *European Journal of Operational Research* 145(2), 382-393.

AGUARÓN, J.; MORENO-JIMÉNEZ, J.M. (2000): Local Stability Intervals in the Analytic Hierarchy Process. *European Journal of Operational Research* 125(1), 114-133.

AGUARÓN, J.; MORENO-JIMÉNEZ, J.M. (2003): The Geometric Consistency Index. Approximated Thresholds. *European Journal of Operational Research* 147(1), 137-145.

ALTUZARRA, A.; MORENO-JIMÉNEZ, J.M.; SALVADOR, M (2005): Searching for consensus in AHP-group decision making. A Bayesian approach. *Proceedings 2nd Compositional Data Analysis, CODAWORK'05*, Gerona.

ALTUZARRA, A.; MORENO-JIMÉNEZ, J.M.; SALVADOR, M (2006): A Bayesian priorization procedure for AHP-group decision making. *European Journal Operational Research* 182, 367-382.

ARNOTT, D.; PERVAN, G. (2005): A critical analysis of decision support systems research. *Journal of Information Technology* 20, 67-87.

BENALOH, J., TUINSTRA, D. (1994): Receipt-free secret-ballot elections (extended abstract). In: *STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, 544–553.

CHAUM, D. (1981): Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24(2) 84–90.

CHAUM, D. (1982): Blind signatures for untraceable payments. In Chaum, D., Rivest, R.L., , Sherman, A.T., eds.: *Advances in Cryptology: Proceedings of Crypto '82* 199–204.

COHEN, J.D., FISCHER, M.J. (1985): A robust and verifiable cryptographically secure election scheme (extended abstract). In: *FOCS.* 372–382.

CRANOR, L.F., CYTRON, R.K. (1996): Design and implementation of a practical security-conscious electronic polling system. *Technical Report WUCS-96-02*, Washington University.

EOM, S.B.; LEE, S.M.; KIM, E.B.; SOMARAJAN, C. (1998): A survey of decision support system applications (1988–1994). *Journal of the Operational Research Society* 49(2), 109-120.

EOM, S.B.; KIM, E.B. (2006): A survey of decision support system applications (1995–2001). *Journal of the Operational Research Society* 57(1), 1264-1278.

ESCOBAR, M.T.; AGUARÓN, J.; MORENO-JIMÉNEZ, J.M. (2004): A Note on AHP Group Consistency for the Row Geometric Mean Priorization Procedure. *European Journal of Operational Research* 153(2), 318-322.

ESCOBAR, M.T.; MORENO-JIMÉNEZ, J.M. (2007): Aggregation of Individual Preference Structures. *Group Decision & Negotiation* 16(4), 287-301.

GARGALLO, P.; MORENO-JIMÉNEZ, J.M.; SALVADOR, M (2007): AHP- Group Decision Making: A Bayesian Approach based on Mixtures. *Group Decision & Negotiation* 16(6), 485-506.

MASLOW, A. (1943): A theory of human motivation. *Psychological Review* 50, 370-396.

McELROY, M.W. (2003): *The new knowledge management : complexity, learning and sustainable innovation*. KMCI Press.

MORENO JIMÉNEZ, J.M. (2003a): Las Nuevas Tecnologías y la Representación Democrática del Inmigrante. En ARENERE, J.*: IV Jornadas Jurídicas de Albarracín.* Consejo General del Poder Judicial. TSJA.

MORENO JIMÉNEZ, J.M. (2003b): Los Métodos Estadísticos en el Nuevo Método Científico. In CASAS, J.M. and PULIDO, A.*: Información económica y técnicas de análisis en el siglo XXI*. Instituto Nacional de Estadística, 331-348. ISBN 84-260-3611-2.

MORENO-JIMÉNEZ, J.M. (2006): E-cognocracia: Nueva Sociedad, Nueva Democracia. *Estudios de Economía Aplicada* 24(1-2), 559-581.

MORENO-JIMÉNEZ, J.M.; AGUARÓN, J.; ALTUZARRA, A.; ESCOBAR, M.T.; TURÓN, A. (2005a): Decisional tools for knowledge improvement in e-cognocracy. In Böhlen et al. (editors): *TED Conference on e-government 2005. Electronic democracy: The challenge ahead*. University Rudolf Trauner-Verlag, *Schriftenreihe Informatik* 13, 70-78.

MORENO-JIMÉNEZ, J.M.; AGUARÓN, J.; ESCOBAR, M.T. (2001): Metodología científica en valoración y selección ambiental. *Pesquisa Operacional* 21, 3-18.

MORENO-JIMÉNEZ, J.M.; AGUARÓN, J.; ESCOBAR, M.T. (2008): The Core of Consistency in AHP-Group Decision Making. Forthcoming in *Group Decision & Negotiation*. DOI: 10.1007/s10726-007-9072-z

MORENO-JIMÉNEZ, J.M.; AGUARÓN, J.; ESCOBAR, M.T.; TURÓN, A. (1999): The Multicriteria Procedural Rationality on Sisdema. *European Journal of Operational Research* 119(2), 388-403.

MORENO-JIMÉNEZ, J.M.; AGUARÓN, J.; RALUY, A.; TURÓN, A. (2005b): A Spreadsheet Module for Consistent AHP-Consensus Building. *Group Decision and Negotiation* 14(2), 89-108.

MORENO-JIMÉNEZ, J.M.; AGUARÓN, J.; TURÓN, A.; SALAZAR, J.L.; PILES, J.J.; RUIZ, J. (2006b): e-Voting process for e-cognocracy. Proceedings *Euro Working Group on Decision Support Systems* (EWG-DSS), London. IRIT/RR-06-14-FR, 51-55.

MORENO-JIMÉNEZ, J.M.; POLASEK, W. (2003): E-Democracy and Knowledge. A Multicriteria Framework for the New Democratic Era. *Journal Multi-criteria Decision Analysis* 12, 163-176.

MORENO-JIMÉNEZ, J.M.; POLASEK, W. (2005): E-cognocracy and the participation of immigrants in e-governance. In Böhlen et al. (editors): *TED Conference on e-government 2005. Electronic democracy: The challenge ahead*. University Rudolf Trauner-Verlag, *Schriftenreihe Informatik* 13, 18-26.

MORENO-JIMÉNEZ, J.M.; SALVADOR, M.; TURON, A. (2005): Group Preferente Structures in AHP group decision making. *Proceedings 2nd Compositional Data Analysis CODAWORK'05*, Gerona.

PILES, J.; SALAZAR, J.L.; RUIZ, J.; MORENO-JIMÉNEZ, J.M. (2006a): The voting challenge of e-cognocracy. Proceedings 2nd International Electronic Voting 2006 Workshop Bregenz, Austria. *GI Lectures Notes in Informatics* P-86, 225-235. ISBN 978-3-88579-180-5.

PILES, J.; SALAZAR, J.L.; RUIZ, J.; MORENO-JIMÉNEZ, J.M. (2006b): Security Considerations in e-Cognocracy. Proceedings 21st Internacional Syposium on Computer and Information Sciences. *Lecture Notes in Computer Science* (LNCS) 4263, 735-744. Springer-Verlag.

ROY, B. (1993): Decision science or decision aid? *European Journal of Operational Research* 66, 184-203.

SAATY, T.L. (1980). *Multicriteria Decision Making: The Analytic Hierarchy Process*. Mc raw-Hill. NY.

SAATY, T.L. (1996). *The Analytic Network Process.* RSW Publications.

SALAZAR, J.L.; PILES, J.; RUIZ, J.; MORENO-JIMÉNEZ, J.M. (2008): E-cognocracy and its voting process. *Computer Standards and Interfaces* 30/3, 124-131.

SIMON, H.A. (1977): *The New Science of Management Decision*. Prentice Hall.