

Digital Democracy and Threats to Privacy*

Nikos FRANGAKIS**

1. Introduction

Much of e-government was initially about the delivery of services and the government's dealings with the private sector, be it the individual (the citizen) or legal entities (the business). But as it has been observed, "you can't build a fence around the citizen as simply a consumer or customer of government services. The same citizen is also an owner or shareholder of government itself. In the digital age, people have an ability to communicate, to participate and add value."¹ Just as the Internet has helped to create a new generation of well-informed and demanding consumers, it will challenge the essentially passive relationship that the majority of people traditionally maintain with government and politics – eventually with Democracy itself. Inevitably, in due course citizens will move from using the web to simply communicate with government, to expecting to enhance through digital means their participation in the public sphere. One day they will expect to be able to cast online votes in a national election.

How soon online voting will become routine is hard to say. But there is more to e-politics and digital democracy than online voting.

Digital democracy could be defined as any electronic exchange in the democratic process, both from the citizens' perspective and from the one of the politicians' and the political system's. It reflects, in this particular ambit, the tendency towards substituting physical participation to politically significant events with using electronic communication means. As well as online voting and voter registration and electoral rolls², digital democracy includes various forms of what could be called "e-participation": opinion polling, campaigning and fund-raising, communication between politicians and voters, Internet political chat rooms, wired legislative bodies, feed back from the public on legislative drafts etc. Apart from governments, political parties and politicians, there are also NGOs, civil society groups, academic institutions, other organisations and individual citizens who are engaging in e-democracy initiatives³, within the broader arena

* This paper is the author's contribution to the 26th International Conference on Privacy and Personal Data Protection, Wroclaw, Poland, 14-16 September 2004.

** Member of the *Hellenic Data Protection Authority*; Managing Partner *Souridakis, Frangakis and Associates Law Firm*; President of the *Greek Centre of European Studies and Research*; Vice-President of the *Hellenic Commission on Human Rights*.

¹ David Agnew, the executive director of the Governance in the Digital Economy programme in Toronto, quoted in: "Digital Democracy" *The Economist* June 22nd 2000.

² Electronic voters registration and electoral rolls are part of e-voting and also a separate item, in the traditional voting process.

³ See *eDemocracy*, Seminar Report, February 12-13, 2004, organised by eGovernment Unit, Information Society D.G., European Commission. See, also, Forum des Droits sur l'Internet (FDI) *Synthèse des contributions sur le forum consacré au vote électronique* (10.6.2003) <http://www.clubpublic.net/evote-forum.php>.

of political marketing. There is no doubt, though, that most initiatives come from the relevant sectors of industry that are interested for more sales of their products...

E-democracy's advocates emphasise as its main advantage the potential re-emergence of citizens' interest for political activity,⁴ as a way to make voting more convenient and attractive at a time of increasing abstention rates and raising low voter turnout. Briefly, the aim could be summarised quantitatively as *more voters* and qualitatively as *more informed voters*.⁵

The introduction of Information and Communication Technologies [ICT] applications in the democratic process could entail a series of threats to the basic democratic principles as defined and protected both by national constitutions and relevant international instruments. Among others, it could threaten citizens' privacy and put at stake their equality in the enjoyment of certain fundamental rights.

E-democracy will inevitably multiply the volume of personal data – including sensitive ones regarding political beliefs and choices – that will be prone to unauthorised transfer and processing. It is therefore imperative for a specific regulatory network of legal protection to be developed.

This paper aims at briefly presenting some of the key issues related to the legal aspects of e-democracy and depicting the related threats to privacy. European views will be taken into consideration, while Greek experiences and approaches will be presented.

2. Constitutional and Legal Requirements

Information society is also *political information society*. Political campaigns are nowadays conducted to a constantly increasing degree by electronic means, while online transmission and simultaneous broadcasting of parliamentary debates and voting enhance the conditions of a virtual “direct democracy”, thus strengthening the sense of participation to citizens. An image of the Parliament being transformed into an immense Εκκλησία του Δήμου [Ecclesia of Demos] is given⁶. The validity of such image is a matter of discussion, but its political impact is undeniable.

According to Community law, if the operation of the democratic system require that, in the course of electoral activities, political parties compile data on people's political

⁴ In a survey of elected officials from 14 European countries, held by the Institute for Electronic Government in 1999, to the question: “*Would you support the introduction of online voting?*” there were 50,4% positive answers as opposed to 30,6% negative ones. To the question: “*Do you believe that information technology can enhance democracy?*” the “yes” was 74,2%, with 15% “no” (see *The Economist*, op. cit.).

⁵ See L.Mitrou, D.Gritzalis, S.Katsikas, G.Quirchmayr, “*Electronic Voting: Constitutional and Legal Requirements, and their Technical Implications*”, in D.Gritzalis (ed.) *Secure Electronic Voting*, Kluwer 2003, p. 45.

⁶ A.Dimitropoulos, “*The Influence of Modern Technology on Constitutional Rights*” in *Revue du droit public et de la science administrative* 2004 225 et seq. [in Greek].

opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established⁷.

All information concerning voting or other politically significant activities is information relating to natural persons (data subjects), according to the definition of article 2 of Directive 95/46/EC and consequently must be treated as protected data. Following the same definition, every piece of information that may lead to the identification of a data subject is personal data, irrespective of the operation(s) leading to the identification⁸. It should be noted that the data in question are, at least *prima facie*, sensitive data as far as they can reveal political opinions, trade union membership, religious or philosophical beliefs and even racial or ethnic origin. Accordingly, data protection principles are applicable: fair and lawful data processing in observance of the finality and proportionality principles, duration of storage and data security appropriate to the risks represented by the processing and the nature of the (sensitive) data to be protected, information and right of access for the data subjects. From the right of access emanates also the e-voter's right to verify if the ballot cast was registered and eventually counted⁹. The provisions of Directive 2002/58/EC¹⁰ particularise and complement Directive 95/46/EC for the purposes of ensuring the protection of the right to privacy, with respect to the processing of personal data in connection with publicly available telecommunication services in the telecommunication networks throughout the Community. Taking into consideration that cookies can reveal a variety of personal information to unauthorised persons and consequently cause privacy threats, their use should be absolutely prohibited not only in e-voting, but even in participatory political activities through Internet, with indicative or advisory purpose. Protection of personal traffic and location data of people taking part in electronic political activities should be covered by adequate measures of security and confidentiality, thus preventing unauthorised access to them or transmission to third parties¹¹. The same applies to surfing or navigation information of the "political" data subjects, since knowing their website visiting habits may reveal their political preferences

Let us now have an overview of the Greek institutional framework. The Constitution of Greece provides that "[t]he deputies shall be elected by direct, universal and secret ballot, by citizens having the right to vote as the law provides [...]"¹². "General elections shall be held simultaneously throughout the State. A law voted by 2/3 of deputies may regulate matters relating to the exercise of the right to vote by electors who are abroad. The

⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23/11/1995 pp 31-50, recitals nos 30 and 36, article 7 (f); transposed in Greece by Law 2472/1997.

⁸ L.Mitrou, D.Gritzalis, P.Donos, G.Georgaroudi, "*e-vote: An Internet based electronic Voting System. Legal and Regulatory Issues on E-voting and Data Protection in Europe*", EU-IST-2000-29518 (D.3.4) p. 35.

⁹ L.Mitrou, D.Gritzalis, P.Donos, G.Georgaroudi, *op. cit.*, p. 41.

¹⁰ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJL* 201/31.7.2002 pp 37-47 – see in particular the definition of "*call*" in article 2 (e). Not yet transposed in Greek law.

¹¹ Directive 2002/58/EC, article 6.

¹² Constitution of Greece, article 51 (3).

principle of simultaneous holding of general elections does not prevent the exercise of voting rights through postal voting or other appropriate means under the condition that the counting and the announcement of elections' outcome is taking place simultaneously throughout the State"¹³. "The exercise of the right of vote is obligatory. [...]"¹⁴. By allowing *other appropriate means*, the Constitution does not exclude, in principle e-voting, as long as it is appropriately organised. An *a fortiori* argument derives from the fact that, after its 2001 amendment, the Constitution has enshrined a series of "electronic rights". The right of everyone to participate in the Information Society¹⁵ and the right to the protection of everyone's personal data¹⁶ are among them. For the time being, though, there has been no legal provision on e-voting, nor any such concrete project in Greece. Legislation on elections and electoral rolls¹⁷ provide for the electronic compilation and storage of the latter but nothing further than that.

3. Threats to Privacy

A general appraisal of the threats privacy is faced with, because of the introduction of digital democracy, will be attempted in this chapter. It should be read, though, in combination with the next one, regarding specific aspects of e-Democracy.

Election-oriented ICT require mass voter authentication, online databases with accurate, up-to-date electoral rolls and voting sites that can withstand concerted hacker attacks. Breaches of secrecy constitute not only a violation of political rights but also an infringement of personal freedoms and privacy rights. Privacy is not simply a refuge for individuals but an expression of self-determination and a prerequisite for the capacity to participate in social and political discourse¹⁸.

The right to keep one's political beliefs and choices secret is an essential aspect of privacy. Voting secrecy has been described as *political privacy*¹⁹. Guaranteeing secrecy, in this respect, means guaranteeing privacy in terms of the data protection legislation. Two potential risks are related: (a) the political opinions expressed by voting or otherwise should not be controlled by public authorities or any other entity or person; (b) nobody should be able to know how one intends to vote or has voted. Voting from home or from the workplace, for example, be it by mail or by Internet, entails the danger that other members of the same family or the employer, respectively, could have knowledge of the content of someone's vote. The French Data Protection Authority [CNIL] has issued negative opinions on three cases where local authorities requested permission for

¹³ Constitution of Greece, article 51 (4).

¹⁴ Constitution of Greece, article 51 (5).

¹⁵ Constitution of Greece, article 5 (2).

¹⁶ Constitution of Greece, article 9A.

¹⁷ See Presidential Decree 351/29-31.12.2003 concerning the codification of legal provisions for the election of deputies.

¹⁸ S.Simitis, "Reviewing Privacy in an Information Society", *University of Pennsylvania Law Review* 135 (1987) 707 et seq.

¹⁹ A.Dix, "Electronic Democracy and its Implications for Political Privacy", in CNIL, *The 23rd International Conference of Data Protection Commissioners*, Paris September 24-26, 2001, p. 369.

experimental electronic voting through Internet for (a) the Presidential Election²⁰, (b) the election of local councillors²¹ and (c) the election of magistrates in labour tribunals (prud'hommes)²². The French Authority's opinion was based on the fact that there was no sufficient guarantee of secrecy and privacy before and during the electoral process, nor satisfactory possibility for effective administrative or judicial control.

Furthermore, CNIL pointed out that an Internet vote that its "material organisation" will depend on technical infrastructure based in New York, escapes from any effective control of the competent national authorities, while the voters' anonymity is forfeited²³.

Under the light of its previous findings CNIL issued a recommendation on the development of the systems of e-voting and the necessary legal requirements to be respected²⁴. It pointed out that e-voting methods and practices are, for the time being, in full development and that the legal requirements for the use of e-voting should be established by legislative means.

The British approach is different: Local authorities are allowed to conduct electoral pilot schemes to test new methods of voting at local government elections. New methods of voting that have been tried as pilot schemes include: e-voting – both using the internet and in special kiosks at polling stations or other public places; telephone voting; voting by text messaging. It should be taken into account that voting by post and, in certain cases, voting by proxy is also permitted in Britain²⁵.

4. Specific Aspects of e-Democracy

4.1. Registration and e-Voting

4.1.1. Registration and Identification

One of the aspects of the voting right is the right to the lawfully exact composition of the electorate. In the context of traditional election procedure, voters are identified and authenticated in the polling station by the use of adequate identification methods based, primarily, on electoral rolls. Electoral rolls constitute personal data filing systems, in the sense of Directive 95/46/EC and nowadays are processed electronically. Provided that their processing is performed in accordance with the relevant legal requirements for the protection of personal data, no threat to privacy can be depicted.

To make reference to some Greek experiences, the Hellenic Data Protection Authority [HDPA] was asked about the amount of data that should be submitted to the local authorities in order for them to compile the electoral rolls and issue the voters' booklets

²⁰ CNIL, Délibération 02-022 du 2 avril 2002.

²¹ CNIL, Délibération 02-090 du 28 novembre 2002.

²² CNIL, Délibération 02-091 du 28 novembre 2002.

²³ CNIL, Délibération 02-022 du 2 avril 2002.

²⁴ CNIL, Délibération 03-036 du 1 juillet 2003, portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

²⁵ See *Ways to vote*, at <http://www.electoralcommission.org.uk/your-vote/waystovote.cfm>.

which ceased to exist in the meantime. Based on the Directive's principles that the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed, the Hellenic Authority excluded the recording of the subjects' spouse's name, profession and home and work telephone numbers as exceeding the purpose of the processing²⁶. In another decision the HDPa stated that a consequence of transparency and publicity of the electoral rolls is the legitimate interest of any voter to check their accuracy and exactness. Such interest obviously supercedes any right or interest of a person the name of whom is listed in the roll²⁷. The necessity of the smooth running of democratic procedures was the grounds for allowing candidates for elected public offices (MPs MEPs, Mayors, Prefects etc) to collect personal data from publicly available sources and process them without being necessary to inform the subject²⁸.

Similarly in Italy the Garante clarified that, as a rule, information must be provided to data subjects if census data contained in public and/or publicly available databases are used for electoral propaganda. The Garante specified that no consent was required if the data were taken from lists, registers and other instruments held by public bodies and freely accessible sources pursuant to laws and regulations (e.g. electoral lists, lists of members of professional associations, or telephone directories)²⁹.

4.1.2. E-Voting

Out of all practical aspects of digital democracy, electronic voting is the most important in the long run, as far as its consequences both for Democracy and Privacy. Elections are significant political events and e-voting constitutes a new mode of participation in the political process, subject to compliance with democratic and constitutional rules of each State. E-voting is not simply an extension of routine Internet applications in commerce and government, but a way to exercise a major political right. It is an online "transaction" where being traceable should be excluded, while verification of authenticity is absolutely essential. Hence, its introduction and acceptance depends on it being done in a way that would guarantee the respect of the principles intertwined with its constitutionally organised democratic nature; therefore it requires a degree of security beyond the current standards for business Internet use. Precondition for this acceptance is the establishment of rules securing the transparency, security, integrity, reliability and the public control and accountability of the process and its actors in a manner that the principles of equality, freedom and secrecy of voting will be fully respected. All information relating to voters, used or processed in an operating e-voting system, should be treated as protected personal data according to the definitions of Directive 95/46/EC, in combination with Directive 2002/58/EC. Briefly, security is not merely a technical issue, but a political one, as well. In order to introduce a widely acceptable and trusted system of electronic voting, additional organisational measures are required.

²⁶ HDPa, Decision no 1123/27.9.2000.

²⁷ HDPa, Decision no 60/2002.

²⁸ HDPa, Decision no 11/2001.

²⁹ 26th International Conference on Privacy and Data Protection, Country Report – Italy.

Any election system may result in unequal access to the electoral process. E-voting could be used to manipulate election results by structuring access in favour of the most Internet-connected and electronically literate. Secure online voting would require not only Internet access, but also additional security means, in order to ensure that the “one voter, one vote” principle, as well as the freedom of voters to form their opinion and to express it, are respected. This includes the free expression, even through casting a non-valid or a “white” paper vote³⁰.

The issues mentioned above that raise justified apprehension over e-voting procedure pertain to remotely voting, such as via Internet, through mobile phones and, in the future, interactive television. They are not related with voting by intranet from traditional ballot stations, since such means of e-voting take place in the presence of election officials and can relatively easily be checked whether they comply with data protection requirements. Nevertheless problems appear even in cases of e-voting at polling sites, as it is the case with voting by touch-screen³¹. The relevant USA experience, particularly after the difficult presidential elections of 2000, cast an widespread doubt over such machines. Critics complain that there is no way to tell if the machines are faulty, insecure or rigged³².

4.2. E-Participation

There is a variety of ICT means enabling citizens to express in real time their views and opinions directly to government, parliament or political parties, thus by-passing mass media that may be controlled by either the government or vested interests.

European institutions use extensively the e-participation tools, in an effort to raise public interest for things European. During the preparatory works for both the Charter of Fundamental Rights and the Convention for the Future of Europe that drafted the Constitutional Treaty, campaigns were extensively publicised in order to attract the wider public’s participation, mainly through Internet. The Greek Presidency of the EU during the 1st semester of 2003 launched *eVote*, a web site subtitled “*Vote for the EU YOU Want?*”. It featured the idea that the responses from people would be incorporated into the daily activities of the Presidency³³.

Among the plethora of ways of political e-participation there are those that do not threaten privacy, such as information web sites regarding elections³⁴, or information on activities of political parties and individual politicians, or direct transmission of parliamentary debates even when the latter take the form of “wired legislative bodies”. There are others where data protection and privacy requirements should be more

³⁰ See L.Mitrou, D.Gritzalis, S.Katsikas, G.Quirchmayr, *op.cit.*, p. 52.

³¹ J.Milarsky and B.Nevins, *Analysis reveals flaws in voting by touch-screen*, July 11, 2004, Verified Voting Foundation, Inc.

³² “The trouble with technology” *The Economist* 18 September 2004.

³³ <http://evote.eu2003.gr/EVOTE/en/about.stm>.

³⁴ It is significant that the web site of the Hellenic Ministry of Interior “*Find out where you vote*” attracted 1.870.000 visits while the relevant telephone switch board only 850.000 calls, during a given period.

carefully taken into consideration. Political chat rooms, campaigning and fund raising are not immune of the threats in question.

Another Greek case could be of interest for the purpose of the present discussion. In February 2004 the (then) governing party requested the authorisation of the Hellenic Authority for the compilation of a registry of its members and “friends”, for the purposes of participating in the nation-wide election of its new president at polling stations designated for this purpose. Members were already filed and could in any event be included in that “electoral roll” by virtue of a special provision exempting political parties, as well as certain other entities, from specific obligations generally imposed by the law³⁵. Regarding the *friends*, though, the HDPA did not allow the electronic filing of their data, since their processing referred to data, prone to reveal the subjects’ political preferences, thus potentially violating the constitutional provision for secret ballot³⁶. It is noteworthy that the voting in question was to be held only a few days before the parliamentary elections³⁷. In compliance with the decision mentioned above, the party amended before the voting its statute, thus effectively assimilating its friends to its members.

5. Conclusions

Information and communication technologies provide significant means, through e-participation and e-voting, to render governing more open, transparent and accountable. E-Democracy may contribute into making democracy more accessible to citizens by increasing participation and involvement in decision-making. Although the number of people dealing with the overall e-Democracy process is still relatively small, its management becomes an important part of the democratic process and therefore should attract the attention of all those who care for democracy.

Many electronic tools, helping political participation and registration and voting are already in use without creating particular problems in relation to privacy and protection of personal data.

E-voting methods and practices by Internet and through mobile phone are in full development. Nevertheless there are several issues regarding the protection of personal data that need to be taken care of, before data protection authorities being satisfied that no serious threats to privacy persist. The legal requirements for the use of e-voting should be established by legislative means and their observance be subject to judicial control. Until such steps are taken, this sort of voting methods should be considered as potentially threatening voters’ privacy.

There is really no reason to hurry towards introducing technological innovations that could cast doubt on their positive result for democracy itself and for the citizen in general. For the time being, substituting physical participation to political events with

³⁵ Law 2472/1997 article 7A paragraph 1 (c).

³⁶ Constitution of Greece, article 51 (3).

³⁷ HDPA, decision no 6/2004.

using electronic communication tools does not necessarily enhance the democratic process, nor does it contribute to better safeguard human rights, including the right to privacy.

*