COMPUTER DEMOCRACY – OUR NEXT STEP IN EUROPE

Tibor Vámos

Introduction

After about a quarter of a century of enlightened development and ongoing preparatory technological, scientific and political activities we are arrived at the realization period of the idea. The two major technological vehicles of progress are the World Wide Web, the most democratic international forum of information exchange and the advent of public key cryptography as a combined philosophical and practical device of individual integrity and collective responsibility.

The Two Major Technological Vehicles

A detailed explanation was given in detail in earlier papers and talks, several ones here in Bulgaria. A short summary to refresh your memory:

www:

- accessible all over the world, even if it is forbidden by (the authorities);
- difficult to trace the receiving user and even the dissemination origin;
- instant information regardless of distance;
- the creation of new groups within a global society;
- provides a stimulus for global standards of reasonable, acceptable, communication among different cultures, a real global human society.

Unfortunately as *Virtue* and *Evil* accompany all human related issues, we meet the *Evil* in:

- terrorism, crime, populist deceptive politicians, people spreading hate, misleading pseudo-science;
- an ocean of information without reliable and well oriented browsing facilities;
- the increasing orientation to business interests and not the original aim of free access to information.

To combat these problems, devoted professional people have developed new tools for elevating the *Virtues* and fighting against the Evil. We, the scientific brotherhood are active, too.

PKC: (public key cryptography)

- defends the individual against all kinds of mishandling of his/her personal data, ideas, views;
- elevates the responsibility and self-defence of the information issuers by preserving an unalterable document of the originally sent message;
- enables legally constituted public authorities to control malevolent information flow;
- enables all active constitutional, legal players in the information flow to control the legal conditions.

These two vehicles create not only technological tools for our global human efforts but a highly general instructive metaphor for future coexistence, the mutual responsibility of different people towards each other and their communities, i.e. a renewed and realistically establish-able *New Agora* in the Athenian, the first drafted but *never substantiated* democracy.

The Current State in Europe

I suppose that you have some more detailed surveys on the subject here, at this conference or at any other meeting devoted to the subject. The best references are collected at the special homepage of e-government. I strongly recommend subscribing to this and join the group of these benevolent people who try to digest an immense and almost impossible amount of information. I am not an agent of this group but for the third year a

happy consumer of their blessed activities and, organizational contacts. This helped us a lot in our successful joining process, which was celebrated on May 1 but prepared during the last quarter of a century.

Indicating the headlines only:

- The efforts are concentrated under the project name: E-2005

  that means a deadline –

  - for adopting standards for EU information; interoperation among the member countries. The IDA project of the EU is the main channel of communication, discussions and setting of standards based on these preparations;
  - for standards of realization on the principles reflected in the PKC ideology, i.e. protection of privacy balanced against the common interest of public democracy and defence of both the individual and communities against mistreatment by terrorism, fraud and political adventurers;
  - creating and distributing technology standards for all these purposes
  - helping people who are handicapped in education, social environment or some other condition to get appropriate support and equal opportunities.
- No EU country can serve as a general and completed standard due to the both highly different traditions of a democratic society and their technological status. In some countries, having a long positive experience in living in a people-serving and autonomous society, people see no problem with a more transparent system based primarily on a single natural identifier. This can be the normal data of domicile or birth register, too. In our kind of countries, people living a long time, i.e. centuries long, under foreign rule, consider the state authorities to be organizations against their civil interests, and traditionally regard underhand dealing as a national virtue. Therefore, they try to defend the individual at any cost against any imaginable governance intrusion.
- The interests of individual and community protection are different and their common view is relative to historical age and type of political system. We can state a positive viewpoint: in the last fifteen years these relations have changed a lot, sometimes also in the minds of the people, especially in that of the younger generations. Technology and experience of protection, and of course inimical actions, have changed even more.
- The EU boards have taken steps to reach a consensus, i.e. appropriate standards according to the technological and psychological possibilities, putting in effect our common constitutional principles. We can learn a lot using the American technology and legislation experience but Europe has its own nearly three millennia experience of its own to reach from, sometimes more tragic, sometimes more human.
- The EU Constitution has accepted currently sets out the general principles outlined in the PKC ideology. Relevant additions should be the separation of personal identification and other data, having a virtual envelop and opening operation. All actions should be registered in a no erasable and no alterable way, monitored by legally elected, independent, responsible bodies. All data unifications should be erased after the action, except the result and the record of the action. All kinds of these data procedures should be permitted by the individuals concerned and communicated to them but the actions of legal authorities (prosecutors and courts) should be carried out under well-controlled legal conditions (e.g. communication of the action only and not the result, time limits for action and secrecy, notification of people for whom the action and the data should be opened or closed).

The Hungarian Story and Experience

The present Hungarian practice is one of the most rigorous in Europe forbidding all kinds of data unifications except those based on prosecutor's or court's decisions. The previous system of a personal identifier (an 11 digit string composed of gender and birth data and a four digit zip code) was abolished though hidden in some way until now by certain authorities. A set of three different and not unified codes was legalized: one for domicile registry (2 characters, 6 digits), one for taxation (10 digits) and one for social security (9 digits). All these happened nearly fifteen years ago, immediately after the fall of the uncontrolled police control system and at a time of very low-level civilian computer usage. The international state of legislative and cryptographic practice

was lower by an order of magnitude and not only the US but the whole world lived before the drama of Sept. 11th and the massive experience of hacker and virus creating operations.

Electronic signature is generally not used though it is legislated. The reason, similar to the general European experience, is the exclusive financial condition: groups receiving the authorization power would like to receive high profits and for justification they started or demanded immense investments for explosion safe buildings, hardware and software systems, all separate for different purposes. The obsolete legislative situation and the particular interests of the different political groups and authorities supported these exaggerated demands.

We have now arrived at a point of almost general consensus for a revision of the early nineties' views and the introduction of current algorithmic software tools. Possessing an excellent school of algorithmic procedures and probability theory we are ready to create a highly safe system. I refer to the schools of Rényi (our academic institute of mathematics recently adopted the name of Rényi) and Erdős.

Politics and Science

Unfortunately, any kind of legislative action largely depends on mostly unintelligent, corrupt, malevolent, erratic politicians and their sycophants in dependent positions. In addition the situation in the daily press is submerging into a tabloid level, even the broadsheet newspapers are more and more interested in scandals and sensational news.

We proposed and partly realized a common effort of all sensible decision makers to unify our forces in a reasonable and given solution. Three branches of the government worked or shifted work and related financial responsibly to each other in the fuzzy channels of bureaucracy. The best educated and experienced, benevolent civil servants stood frustrated within the whirl of irresponsible politics.

The Academy of Sciences, being a partly independent and respectful body tries to convince the responsible decision making persons to consider national interest as a higher principle than their own financial and power involvement. The Committee, appointed by the President of the Academy includes outstanding personalities in the legal, social, computer related sciences, senior figures of our information history and the Ombudsman of data protection, who should be independent of political parties and elected by the Parliament. No active politician or government administrator is among the membership to maintain the Committee's political independence as a body. The Committee has no claim for any intervention but works with all state related people and organizations that are willing to do so.

I would like to mention that we found in a small minority of politicians several devoted and able people, who joined political groups in the hope of improving the regrettable situation. However, they all are subdued by the overpowering, negative influence of the more aggressive unscrupulous powers. These positive actors, sitting on both sides of the political divide welcomed the initiative of the Academy and are meaningfully cooperating with us.

We have had to experience the disastrous influence of political splits in relevant non-political problems and the dysfunctional organization of the political system, in its personal selection constraints and in overburdening practice, extending political and administrative activity far beyond the really necessary principal tasks. The operation stimulated thinking about the revision of state administration practice, returning to much older ideas of democratic and professional governance by adoption of both new tasks and technologies.

According to our observations, similar problems arose in every developed country and organization, even in multinationals and other international bodies. Thus the problem is less an issue of unrealistic ethical philosophical judgement but much more a social, cultural and organizational issue, i.e. an information science related question of our age and our intellectual communities.

A consensus of relevant thought in the legal profession has now been reached. Those who were pioneers of our present democratic constitutional order advocate the need for rational revision and that provides additional support of the need, as a priority, professional quality in all public affairs. We refer to the great Greek thinkers on city-governance (πολιτεια) especially *Aristotle* and the funeral speech of *Pericles*, reported later by *Thucydides* and to the *Founding Fathers* of the US through, their essays and papers in the *Federalist*. From the 19th century we have also had a wonderful tradition in Hungarian history, starting with the *Sage of the Country by,* Ferenc Deák.

The Proposal of the Hungarian Academic Committee

The proposal is clear:

- for the equal opportunity of citizens the right for electronic signature on an equitable basis, i.e.
  - it should be given free of charge for those whom it is a financial burden and not expensive for anybody. (.e.g. in relation to the taxation system)
  - electronic signature should be the only required authorization for any kind of public activity. If possible, this should be extended to banking operations, too;
  - all public authorities should participate in the popularisation, education and, training of different layers of society for usage and for being conscious of one's rights;
  - the state and, all accountable public authorities related to the electronic signature issue should be responsible for the preservation of the Civil Rights of individual citizens and any of their respective legal groups.

The measures are detailed above and should follow the agreements of the EU. EU conformity is the basis of interoperation and is a constitutional requirement. According to our legal experts this requires no fundamental change in our legal system, only some further updating and corrected interpretations, and the constitutional empowerments for participation in the EU.

- Technological means should not be included in the legal regulations, the system must be flexibly open for any kind of realization, i.e. currently traditional authorized handwriting, smart card, SIM-card used in mobile systems, biometrical (fingerprint, fundus, DNS, etc.) data.
- The Law should take care of independent and open operational authorities prescribing algorithms, the code length for citizens and prosecution and, other safety conditions related to data and their handling personal.

Going Together – Neumann and Athanasoff – Iliev

Bulgaria and Hungary have much common ties in our history, beginning with the Huns for those who believe the Hungarians are the successors of Attila and the ancient Bulgars who are really supposed to be the descendants, with lesser and greater Byzantine influence, with the tragedy of a certain city called Varna in 1444, with Turkish, German and Russian domination but most important of all should be the future, based on another lesson: of Neumann and Athanasoff.

Both were pioneers of the computer age, Neumann in mathematical and logic theory, Athanasoff more in technology. Neumann had to leave his country to avoid being a victim of the Holocaust, Athanasoff's family left for a better life, both, subsequently, had more possibility to develop their genius.

Now we enter a new age, based on our common three millennia old European history and, hopefully, our talent find a home within a more peaceful, less hatred-contaminated world, preparing a common home for our descendants. I remember here my friend Lubomir Iliev who passed away not too long ago and was not only a great mathematician and teacher of computer science but, at the same time, a representative of European cultural tradition and values. We always considered the two be inseparable by regarding these subjects as both metaphors and parallel realities.

These are the main lessons of that progress: preserving individual values within a cooperative, empathy driven human community. Let us hope that this comes true!

Author Information

Tibor Vámos – Computer and Automation Research Institute, Hungarian Academy of Sciences, H-1111 Budapest, Lágymányosi u. 11, Hungary; e-mail: vamos@sztaki.hu