LEGAL INFORMATICS AND e-GOVERNANCE AS TOOLS FOR THE KNOWLEDGE SOCIETY

Erich Schweighofer (ed.)

Prensas Universitarias de Zaragoza

LEFIS
LEGAL FRAMEWORK FOR THE INFORMATION SOCIETY

FICHA CATALOGRÁFICA

LEGAL Informatics and e-Governance as Tools for the Knowledge Society / Erich Schweighofer (ed.). — Zaragoza : Prensas Universitarias de Zaragoza, 2008
199 p. ; 22 cm. — (LEFIS Series ; 2)

ISBN 978-84-7733-984-7
1. Informática–Derecho. I. Schweighofer, Erich. II. Prensas Universitarias de Zaragoza. III. Serie: LEFIS Series (Prensas Universitarias de Zaragoza) ; 2
34:004

1.ª edición, 2008

Ilustración de la cubierta: David Guirao

Prensas Universitarias de Zaragoza. Edificio de Ciencias Geológicas, c/ Pedro Cerbuna, 12. 50009 Zaragoza, España. Tel.: 976 761 330. Fax: 976 761 063
puz@unizar.es http://puz.unizar.es

Prensas Universitarias de Zaragoza es la editorial de la Universidad de Zaragoza, que edita e imprime libros desde su fundación en 1542.

Impreso en España
Imprime: Servicio de Publicaciones. Universidad de Zaragoza
D.L.: Z-606-2008

TABLE OF CONTENTS

PREFACE

In this first decade of the new millennium, government has turned into e-Government: all agencies now draw heavily on increased use of information and communication technologies.

This book publishes the results of the LEFIS Seminar on Legal Informatics and e-Governance as tools for the Knowledge Society that took place in July 2007 in Reykjavik, Iceland.

The LEFIS group comprises different disciplines of science providing a strong interdisciplinary view on this subject. Thus, the contributions cover the following topics:

— General questions
— Technology
— e-Administration
— e-Justice
— e-Governance in less advanced States.

The chapter 'General questions' starts with an introduction into e-Government in the information society presenting the main concepts of governance in cyberspace: e-Persons, e-Transactions, e-Documents and e-Signatures. The next article deals with the question who controls and who is controlled within e-Governance, e.g. regimes of technological power. Habermas and Foucault seem to be alternatives as e-Government instruments support on the one hand a broad institutionalisation of a discourse, otherwise enable also control degrees not known before.

The chapter 'Technology' starts with ontologies. As regulation is increasingly complex, new tools for easy access, understanding and applying these rules are required. Ontology-based content management systems can improve the quality and efficiency of the knowledge processes. Further, a semantic web tool for electronic manipulation of European texts about conflicts of jurisdiction is presented. The third contribution deals with other than Latin domain names on the Internet. As the number of Internet users grow, demand for non-Latin domain names is increasing. At the moment, the feasibility of IDN is further tested.

The chapter 'e-Administration' focuses on e-Identification and the new developments in Bulgaria. Registries, e-Documents, e-Signatures and e-Government have been introduced in Bulgaria. However, the implementation proves to be much more work than expected leading to delays.

The first contribution of the chapter 'e-Justice' describes the progressive implementation of new technologies in the administration of justice in Spain: video documentation, electronic bracelet, judicial MEMO and videoconference. The next article deals with the technological development in Italy. Last, a short overview on the situation of e-Justice in Bulgaria is given.

In the last chapter on 'e-Governance in less advanced States', e-Societal Management (e-SM) and its role in socio-economic development is described.

Last but not least, I would like to express my thanks to Fernando Galindo, University of Zaragoza, for organizing the workshop in Reykjavik and his support for this book. Further, thanks are due to the authors for their contributions that cover a broad range of e-Government questions from the point of view of law.

Wien/Bruxelles, September 2007 Erich Schweighofer

CHAPTER 1
GENERAL QUESTIONS

e-GOVERNANCE IN THE INFORMATION SOCIETY

Erich Schweighofer[1]

1 Introduction

The goals of the legal order as a system of social rules with sanctions are stabilisation of behaviour[2] and risk reduction.[3] Information society does not change these aims, however, the methodology of law has to adapt to the new concepts of the 'electronic' environment: governance of cyberspace instead of territorial sovereignty, e-Persons as 'electronic realisation' of persons and e-Transactions as the main form of human action (e.g. e-Government, e-Commerce and e-Democracy).

An information society is a society which makes extensive use of information and communication technologies, produces large quantities of information and communication products and services, and has a diversified content industry.[4] The change from the

---

1 University of Vienna, Centre for Computers and Law, Schottenbastei 10–16/2/5, 1010 Wien, Austria, <erich.schweighofer@univie.ac.at>. Presently on leave; working for the European Commission in Brussels. The expressed views are those of the author.

2 N. Luhmann, *Vertrauen – ein Mechanismus der Reduktion sozialer Komplexität*, 1968.

3 'Living dangerously, A survey of risk', *The Economist* (London), January 24th 2004.

4 This definition is based on the OECD model that sets statistical standards for measuring the information society. OECD, *Working Party on Indicators for the Information Society, Guide to Measuring the Information Society*, Paris, 2005, <http://www.oecd.org/ dataoecd/41/12/36177203.pdf> (visited 13 September 2007).

industrial society to the information society is characterised by a transition from an economy based on material goods to one based on knowledge.[5]

With the Internet, a global infrastructure for the exchange of information and communication exists that determines the society based on knowledge. A global village has been created without borders.

Cyberspace, after been a metaphor for a new space in which through communication and data transfer certain actions are set,[6] has got a quite useful legal definition by the US Supreme Court in 1997:[7] '[…] a unique and wholly new medium of worldwide communication. […] Taken together, these tools [email, mailing list servers, newsgroups, chat rooms, World Wide Web] constitute a unique new medium – known to its users as "cyberspace" – located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet'.

It has to be mentioned that cyberspace is not yet virtual reality; it primarily concerns interaction over computer networks, in particular over the Internet. Like its synonym 'information highway', it refers to interactive electronic communication consisting of a whole range of informational services.

2 Governance in Cyberspace

Governance is defined as the exercise of political authority and the use of institutional resources to manage society's problems and affairs.[8] Legal governance means the rule of law for efficient risk reduction of

---

5 P. Drucker, *The Age of Discontinuity*, London: Heinemann, 1969.

6 W. Gibson, *Neuromancer*, New York: Ace Books, 1984; E. D. Reilly (ed.), *Concise Encyclopedia of Computer Science*, Chichester: Wiley, 2004, pp. 221 et seq.; N. Negroponte, *Being Digital*, London: Hodder & Stoughton, 1995.

7 United States et al. v. American Civil Liberties Union et al. (1997).

8 World Bank, *Governance Matters, Worldwide Governance Indicators*, 2007; <http://info.worldbank.org/governance/wgi2007/home.htm> (visited 13 September 2007).

social behaviour by providing legal security. Such definitions are based on the Westphalian system of 1648 of territorial sovereignty.[9] However, in the information society, territorial boundaries are becoming more and more superfluous as high transport capacity and new forms of communication like the Internet have severely limited the possibilities of borders.[10] It has become very difficult or even impossible for a state to cut oneself off from the practice of other States.[11] Thus, States have to consider limitations to their territorial sovereignty. The liberal approach of sovereignty[12] places human beings and associations of civil society in the centre of international relations. Sovereign rights of men may be transferred to various regulation providers whereas the most import one will be, without doubt, the territorial state. A new transnational order will be established that is characterised by increased international networking of persons, private organisations, commercial enterprises and various entities of government.

The regulation of the cyberspace in the information society constitutes a major part of global governance. 'Governance is the sum of the many ways individuals and institutions, public and private, manage their common affairs. It is a continuing process through which conflicting or diverse interests may be accommodated and co-operative action may be taken. It includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions either have agreed to or perceive to be in their interest'.[13] Global governance can be defined

---

9 Cf. H. H. Perritt Jr., 'The Internet as a Threat to Sovereignty: Thoughts on the Internet's Role in Strengthening National and Global Governance', *IJGLS*, vol. 5 (1998), <http://www.law.indiana.edu/glsj/vol5/no2/4perrit.html>; H. H. Perritt Jr., 'The Internet and International Law', *Kentucky Law Journal*, vol. 88 (1999–2000), no. 4, pp. 885–955.

10 Ch. Engel, 'Das Internet und der Nationalstaat', *Berichte der DGVR*, 35 (2000), pp. 353–425.

11 W. B. Wriston, Bits, 'Bytes and Diplomacy', *Foreign Affairs*, September–October 1997, pp. 172–83.

12 A.-M. Slaughter, 'International Law in a World of Liberal States', *EJIL*, vol. 6 (1995), pp. 503–38.

13 *The Report of the Commission on Global Governance*, Oxford: Oxford University Press, 1995, chapter 1.

as 'collective efforts to identify, understand, or address worldwide problems that go beyond the capacity of individual states to solve'.[14]

The idea of a separate cyberspace jurisdiction of mid-1990ies[15] has not got acceptance. Cyberspace remains a space where states jurisdictions apply according to complex public and private international law rules leaving some lacunas due to non-regulation (or better regulatory restraint)[16] or conflicting regulatory approaches (e.g. data protection, pornography, lotteries, spam or nazi-propaganda).

This complex picture of regulation can best be structured by using the concept of regulation agents.[17] States (territorial sovereignty, personal sovereignty or unilateral regulation), governmental international organisations, non-governmental international organisations, transnational corporations, associations of civil society compete for regulation in this regulation space, however, without question, leaving the territorial state the most prominent role.

The regulation is characterised by the end of strict hierarchies (governance by government), the competition of different regulation systems (governance with government), a strong transnational order[18] with new forms of regulation like regimes, network or self-

---

14 R. Thakur and T. G. Weiss, *The UN and Global Governance: An Idea and its Prospects*, <http://www.unhistory.org/publications/globalgov.html> (visited 13 September 2007).

15 D. R. Johnson and D. G. Post, 'Law and Borders. The Rise of Law in Cyberspace', *Stanford Law Review*, vol. 48 (1996), p. 1367.

16 K. W. Grewlich, *Governance in Cyberspace*, The Hague: Kluwer Law International, 1999.

17 C. Kirchner, 'Informationsrecht: ein institionenökonomischer Zugang', in Jürgen Taeger and Andreas Wiebe (eds.), *Informatik – Wirtschaft – Recht. Regulierung in der Wissensgesellschaft. Festschrift für Wolfgang Kilian zum 65. Geburtstag*, Baden-Baden, 2004, pp. 103–16; D. Johnson, S. Crawford and J. Palfrey Jr., 'The Accountable Net: Peer Production of Governance', *The Virginia Journal of Law and Technology*, vol. 9 (2004), <http://www.vjolt.net/archives. php?issue=19> (visited 13 September 2007); E. Schweighofer, 'A Review of ICANN's Uniform Dispute Resolution Policy', *Austrian Review of International and European Law*, Kluwer Law International, vol. 6 (2001), pp. 91–122.

18 P. C. Jessup, 'Transnational Law', *Vanderbilt Journal of Transnational Law* (1956).

regulation, the exit option of citizens, companies and communities and a governance by recognition characterised by limited enforcement possibilities of the territorial state.

3 e-Governance

The concept of e-Governance has two main meanings. On the one hand, it refers to the regulation of the use of information and communication technologies (ICT). This part is called ICT law or information law and will not be addressed in this contribution.[19] On the other hand, it concerns using ICT for governance that requires the introduction of new concepts of governance: e-Person and e-Transaction.

Human beings must have an electronic identity (e-Person). In the cyberspace, these e-Persons will act via e-Transactions, e.g. acts of information and communication.

It is astonishing how wide e-Transactions can be used to supplement or even substitute actions in real life. So far, the full potential is still developing. The various activities can be clustered into e-Government – doing government on the Internet, e.g. offer information and services for citizens and businesses on the Internet –, e-Commerce – doing business on the Internet, e.g. offer products and services on the Internet –, e-Democracy – doing voting and giving participation on the Internet –, and e-Entertainment and e-Life (second life) – living and enjoying live on the Internet.

4 e-Persons

In cyberspace, traditional identification of legal persons must be extended by the concept of e-Persons.[20] Persons are still human beings

---

19 I. J. Lloyd, *Information Technology Law*, fourth edition, Oxford University Press, 2004.

20 E. Schweighofer, 'Vorüberlegungen zu künstlichen Personen: autonome Roboter und intelligente Softwaareagenten', in E. Schweighofer et al., *Auf dem Weg zur ePerson, Aktuelle Fragestellungen der Rechtsinformatik 2001*, Wien, Österreich, 2001, pp. 45–54.

but, contrary to real life context is quite often excluded in cyberspace transactions due to the very limited wits level, in input as well as in output. Acting as a person in cyberspace means having a name (or a pseudonym), and having an electronic identity, e.g. a data entry in a trustable register like a credit card number, a Bancontact/ ATM/Maestro card, an e-mail, an IP number, a domain name, a telephone number, Skype identity, E.NUM, or, like in Austria, a source identification number (*Zentralmelderegister-Nummer, Stammzahl*[21]). The problem of identity link, some sort of a 'biometric touch', exists and is faced mostly by secrete information (user identity, pass words, PIN/TAN codes, electronic signatures, etc.), sparsely so far by finger prints, IRIS scans, genetic data or RFID chips. In practise, the concept of e-Persons works surprisingly quite well, however, also allowing new forms of crime like personality theft.

e-Persons are another extension of the activity options of human beings like intelligent agents or robots.[22] Intelligent agents are software programs acting for a human being or another program in a relationship of agency in cyberspace. Robots are electromechanical systems in real world that can sense and manipulate its environment. In both cases, legal systems have to consider giving intelligent agents or robots some form of 'limited' legal personality in order to allow the application of the concepts of representation and responsibility.

5 e-Transactions

The term of e-Transaction covers all human actions possible in cyberspace, e.g. what can be done with the limited options of action in that space. Thus, 'only' actions consisting in information and

---

21 Section 6 of the Austrian e-Government Act, Federal Law Gazette (*Bundesgesetzblatt*), part I, no. 10/2004; <http://www.cio.gv.at/egovernment/law/E-Gov_Act_endg_engl_Fassung1.pdf> (visited 13 September 2007).

22 T. Christaller et al., *Robotik. Perspektiven des menschlichen Handels in der zukünftigen Gesellschaft*, Berlin: Springer, 2001.

communication are possible. Typical actions are active and passive communications and database transactions. On the side of the service provider on the Internet, databases are predominantly the tool for offering goods and services.

In the days of terminal and mainframe computer communications, such traffic of data was impossible. Network infrastructure and communication techniques had to undergo a major revolution in order to deliver gigabits per second to the user.[23] These changes had to include public data communications networks such as the Internet allowing real-time networked multimedia.

A communication transaction is an exchange of information.[24] Parties of a communication must have a common language that can be auditory (speaking or singing), nonverbal, physical (body language, sign language, paralanguage, touch, eye contact) or writing. The process of information transmission is governed by syntactic (formal properties of signs and symbols), pragmatic (relations between signs/expressions and their users) and semantic rules (relationships between signs and symbols and what they represent). The syntactic rules consist of the package of communication protocols TCP/IP, of HTML and XML and applications based on these standards. Whereas major improvement can be noticed over the years, syntax still strongly limits transactions compared to real life. It should also be mentioned that this communication part is regulated on a global level via the Internet Corporation for Assigned Names and Numbers (ICANN).[25]

Regulating of this communication beyond the syntactic level still remains the prerogative of the states. Legal systems determine by pragmatic and semantic rules how communications over the Internet may be done or not.

---

23 Reilly, footnote 6, pp. 225 et seq.
24 *Wikipedia, the free encyclopedia*, 2007 (visited 13 September 2007).
25 Schweighofer, footnote 17.

A database is a collection of interrelated data of different types.[26] Data values are subject to validation conditions. Data organization follows mostly the relational approach.

A database transaction is a unit of interaction with a database management system or similar system. It is independently handled from other transactions a coherent and reliable way. Characteristics are atomicity (transaction must be either completed or aborted), consistency, isolation and durability.[27]

In databases, transactions can be allowed either anonymous or requiring identification (e.g. user identity and password). On the Internet, only an often dynamically created IP address is sufficient for access. For doing e-Government or e-Business, more identification is required, in particular e-Signatures.

In law, most transactions can be done via electronic information and communication if persons are properly identified. No real limits exist in practise for negotiations, concluding agreements or court actions. However, requirements of immediacy, of personal contacts, of personal evaluation and the like reduce the practical implementation of legal e-Transactions. e-Government or e-Justice reduce barriers and will lead to much bigger acceptance. Budgetary constraints and demands of higher efficiency are strong catalysers for this development.

All legal e-Transactions can be combined in the concept of e-Document. Here, a short abstraction is necessary. Human behaviour like negotiations, conclusions of contracts, applications, notices, court actions, court hearing, etc., still remains as such. As it is common to summarize these actions in documents, nowadays such tasks are done by e-Documents with the advantages of easier communication or sharing of information. Whereas text remains the standard, in the future, videos will strongly gain higher acceptance.

---

26 Reilly, footnote 6, pp. 245 et seq.; C. J. Date, *An Introduction to Database Systems*, 8th edition, Reading, MA: Pearson Addison–Wesley, 2003.

27 *Wikipedia, the free encyclopedia*, 2007 (visited 13 September 2007).

It is quite obvious that e-Delivery of services does not constitute an e-Document but an e-Action in real world. For example, delivery of information, banking services or entertainment are handled in such a way with significant cost savings.

6 e-Documents and e-Signatures

Legally relevant communication is focussed on e-Documents. The document (in Latin: *documentum* = proving certificate) is any discrete representation of meaning (in law in particular: will or statements). e-Documents mean the replacement of a written document by a file, e.g. a 'virtual' document in electronic (digital) format.

In the digital word, every copy is the same as the original. Thus, the requirements of a written document, authenticity (prove that the document remains unchanged) and identity (prove that the document origins from its producer), have to be differently solved than in the 'Gutenberg age'.

Hash functions reduce files to an essentially unique digest. Each change of the document leads to a change of the hash function. Therefore, authenticity can be guaranteed but avoiding that each block of a long message has to be signed individually.

Combined with certification, e-Signatures establish the identity of the producer of an e-Document. The most commonly used standard RSA[28] allows both functions. Documents are signed by the producer with his private key, whereas the public key allows verification by others that the producer has actually signed this document. Certification authorities keep a register of signature certificates and public keys. Thus, an e-Signature constitutes an electronic identity card of the owner.

---

28 R. L. Rivest, A. Shamir and L. Adleman, 'A Method for Obtaining Digital Signatures and Public-key Cryptosystems', *Communications of the ACM*, 21/2 (1978), pp. 120–126.

In some jurisdiction, e.g. the Austrian one, the e-Signature is combined with special identification, the so-called SourcePIN number, a unique identification number for citizens and residents in Austria.

The standard on e-Documents and e-Signatures described above is a quite high one. In practice, it is still not sufficiently established that such a high standard is required for all written documents. Practice shows that a less sophisticated standard might have higher penetration without significant lower risks.

An example of this discussion: The Austrian e-Government contains a transitional provision that so-called administrative signatures shall be treated in the same way as qualified signatures (e.g. signatures following Article 5.1 of the Directive 1999/93/EC). With a proposed amendment in 2007, this provision shall be extended up to 2012.[29] It should also be mentioned that banks in Europe mostly still use PIN/TAN codes (or similar systems) and not e-Signatures.

Thus, a risk analysis should be the decisive factor for finding appropriate security levels of e-Signature. Quite often, possession of certain cards and information has proven to be sufficient (e.g. e-Commerce with credit card information). This approach may be also possible for the public sector, provided that sufficiently strong identity links are established.

7 Conclusions

Governance in the information society has some particularities in comparison to territorial governance. Firstly, due to the global nature of the cyberspace, governance has to be global. Secondly, due to the lack of a global authority, governance is handled not only by one

29 Proposed amendment of the Austrian e-Government-Act: 96/ME (XXIII. GP): *Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, Änderung* (e-GovG-Novelle 2007); <http://www.parlament.gv.at /portal/page?_ pageid=908,6640640&_dad=portal&_schema=PORTAL> (visited 13 September 2007).

territorial State by a number of governance providers of which concerned States remain the most important ones. Thirdly, governance has to include other methods than law for stabilising human behaviour, in particular the so-called 'soft law'. The change in the relevant concepts of regulation, marked by *e-* in the names, in particular e-Persons, e-Transactions, e-Document and e-Signatures, has to be well understood in order to create an efficient legal order in cyberspace.

In Europe, the legal framework for the information society is already quite properly established. However, still important fine-tuning has to be done in practice in order to incorporate these new concepts in the existing legal orders.

A JANUS-FACED VIEW OF THE ELECTRONIC GOVERNANCE. BETWEEN FOUCAULT AND HABERMAS

Karol Dobrzeniecki[1]

1 Introduction

To the pantheon of the ancient Romans, besides well known, powerful gods like Jupiter, Juno or Minerva, belong also less popular, modest and sometimes almost forgotten divinities. One of them is a two-faced Janus, god of transitions, gates, beginnings and endings.[2] This article refers to him in a very metaphorical sense.

God Janus will be hereafter utilised as a leitmotiv for interpreting and evaluating new modes of coordination of social behaviour emerging at the turn from the industrial society to the informational society. In order to do that I refer to two famous social thinkers of the twentieth century: Jürgen Habermas and Michel Foucault. Their ideas are like two faces of Janus, two different points of view of electronic governance being the core of a digital revolution.

---

1 Nicolas Copernicus University, Faculty of Law and Administration, ul. Gagarina 15 87–100 Torun, Poland, <karol.dobrzeniecki@law.uni.torun.pl>.

2 He used to be worshipped at the beginnings of the harvest and planting, marriages, births, etc.

2 Postmodern times, new technologies and transformations within the mechanisms of control

Putting aside the heated debate about the essence of postmodernism, its sufficient working definition may be as follows. Postmodernism is a set of beliefs both with a cultural environment in which the beliefs occur. Characteristic features of its cultural artefacts are fragmentation, diffusion and 'emphasis on surface'.[3] Dominating style of pastiche, irony, and mediazation of messages and symbols makes postmodernism an *époque* of paradoxes. In this article an example of such paradoxes will be elaborated.

The expansion of electronic means of communication has double impact on the human liberty. Popularisation of ICT (information and communication technologies) tools extends the sphere of personal freedom by breaking the barrier of time and distance. Unfortunately, by the same facts it enables surveillance and control on a scale inconceivable up to then.

It brings us to the point in which the title term of electronic governance should be introduced. It denotes the sum of various mechanisms used for coordination of human activities in which ICT are essentially involved. This relatively new phenomenon has occurred as a consequence of some recent events. Two of them should come under closer scrutiny. The first thing is privatisation and trans-nationalisation of governing competences traditionally tied to a state. As a result of these processes the sharp distinction between states and markets and between the public and the private is being lost. The second event to be considered is a massive digitalisation and computerisation of almost all dimensions of a social and individual activity.

---

3 Balkin (1991–2).

Transformations within the mechanisms of social control manifest themselves in a shift from solely legal regulation to pluralistic and heterogeneous governance. In the last decades of the 20th century the traditional state monopoly to exercise power was limited substantially. It is related with the fact that states have to take into account the increasing autonomy of numerous organisations and institutions that operate within its territory. The control based exclusively on state law is marginal to contemporary processes of ordering, which involve activities of individuals and institutions, public and private. The regulatory control is diffused through society. State law is only likely to be effective when linked to other ordering processes.[4] Helmut Wilke has correctly noticed that the contemporary times have forced states to take seats at negotiating tables.[5]

Also new concepts of governance are developed at the supranational level. One of them is 'transgovernmentalism'. In this vision global governance is taking place through global networks of national government officials which are flexible, often informal and may response spontaneously 'to the need to interact to coordinate policy and address common problems'.[6] Their activities are usually not strictly controlled or closely guided by the national governments and in this aspect differ from the traditional regime of international relations.

In the legal theory the principle of monocentrism is gradually replaced by the principle of multicentrism. Many outstanding representatives of jurisprudence, e.g. Neil MacCormick, have started defining law in a new way. This approach negates the existence of any analytically necessary nexus between law and state. In MacCormick's opinion Kelsen was wrong asserting that every state is by itself a 'law-state'.[7] Similarly, state law is just one form of law, in a sense it belongs to the family of institutional normative orders, but surely is not the only one. State law dominated in particular

4 Scott (2005).
5 Wilke (1983).
6 Slaughter (2002–3).
7 Kelsen, *Pure Theory of Law*, Berkeley: University of California Press, 1967.

historical circumstances but there is no necessity and certainty this situation will last forever. The coming world order may therefore be built beyond the sovereign state, which prominent contemporary examples are a development of legal order under the European Convention on Human Rights and within the European Union. Within the range of our acquaintance there are also ecclesiastical law of various churches, law of organized sports and games, etc. In this pluralistic conception of legal system 'distinct systems can coexist without any one having to deny either the independence or the normative character of another'.

According to MacCormick objectively valid normative orders may give conflicting answers to the same point without necessarily being any specifically legal method for eliminating the conflict. His theory allows a situation in which an individual's legal position is becoming a matter of inquiry into more than one normative order. Possible conflicts between them will simply go unresolved or their resolution may be a matter for political rather than legal processes.[8]

What also differs thinking in terms of governance from traditional legal reasoning is another approach to the deployment of power for the purposes of governing. It does not assume that the only useful form of power is political power based on sovereignty. Sources of power derive from information, wealth and organizational capacities. For example designing buildings or software may also be applied in order to control behavior.

More and more often in public debates it is spoken about 'managing common affairs' by formal or informal arrangements instead of enforcing an officially adopted set of norms within a particular social field. It may be interpreted in such a way that sovereign law is being displaced by other modalities of power. One of them is 'disciplinary power' discovered by Michel Foucault.

There are disparate practices and technologies which control and govern in contemporary global society. Many of them may be linked

---

8 MacCormick (1996–7, 1998–9).

with recent revolutions in telecommunication and computer sciences. A great progress within the information and communication technologies has shaped a new kind of social organisation denoted by popular terms such as 'knowledge society', 'informational society' or 'network society'. Their common semantic core concerns the social transformation caused by new information technologies. Manuel Castells has distinguished constitutional features of an information technology paradigm which are the material foundations of such a type of society. Firstly, it is an invention and popularisation of technologies that act exclusively on information by processing data. It leads to a situation that almost all processes of individual or collective existence are directly shaped by the new technological medium. Additionally, growing convergence in IT sector takes place. Old, separate technological trajectories become literally indistinguishable. Interconnected IT tools form one logical network. A morphology of the network is well adapted to increasing complexity of a social system using these technologies. In such a society rules may be fundamentally altered without destroying the social organization because the material basis of the organization can be reprogrammed and retooled.[9]

The setting of power relations observed in the IT sector confirm a thesis that nowadays capacities and resources relevant to the exercise of power have dispersed among a wide range of state, non-state and supranational actors. Non-state rule makers are very active in the field of standard-setting and normalization. Private standards bodies receive state support both 'through funding and through the incorporation of standards into legal regulatory requirements. Private standards are also rendered effective through their incorporation into contracts'.[10]

The above events make the electronic governance a challenge for traditional theory of the regulation based on legal positivistic approach.

---

9 Castells (2000).
10 Scott (2005).

3 Why a theoretical deliberation over the electronic governance?

My intention in this article is to place the problems of electronic governance in a philosophical perspective. Such a dimension should be identified and developed. First, we need to overcome thinking in terms of technological determinism. One leads to an acceptance of the fatality of the situation where technology is an autonomous force that shapes society and causes social change. People are forced to organize themselves to meet the needs of technology. The outcome of this organization is beyond their control. Determinists claim technology is a key governing force in society, which merely has to adapt to it. Overcoming a technological determinism means to wake up other existing social forces in order to take control of the direction in which society develops, not just passively participate in a so-called 'technological progress'. There is a necessity to find out what kind of interdependence exists between new information technologies and social life, to what extend human values, choice, and ideas must be dominated by technique. Then there will be a need to institutionalize firm forms of social and moral control over the path of innovation and the consequences of technology for humans.

The other reason for the theoretical approach is a problem of a conceptual vacuum. James H. Moor has noticed that automatic application of traditional ethical theories to generate the appropriate policy within the IT sector is usually not possible.

> Although an ethical problem may seem clear initially, a little reflection reveals a conceptual muddle. What is needed in such cases is an analysis which provides a coherent conceptual framework. […] Let's suppose we are trying to formulate a policy for protecting computer program. Initially, the idea may seem clear enough. But then a number of questions which do not have obvious answers emerge. What exactly do these terms mean? Many technological issues must be clarified in order to formulate a useful policy. The conceptualization will not only affect how a policy will be applied but to a certain extent what the facto are.[11]

11 Moor (1985).

The electronic governance has also to face one more challenge. New technologies provide members of society with new possibilities for acting, thus new values emerge. Digitally processed information has a value in the present culture it didn't have a few decades ago. On the other hand old, well known values have to be reconsidered in the new circumstances, e.g. importance of the protection of intellectual property rights and their influence on the freedom of speech.

4 Information, communication and philosophy. Reference to Habermas and Foucault

By constructing a philosophical dimension of any phenomenon, acts of inclusion and exclusion must be performed. It refers to particular opinions, theories, schools of thought or even whole philosophical traditions. In this assay only two social thinkers were chosen to be utilised as founding fathers of the electronic governance theory. The whole galaxy of excellent philosophers was passed over. This difficult choice was determined by the fact that both of them have stressed the importance of the language as a final architect of every process of socialisation. It makes their works well suited to assessing the phenomena of digital revolution, which has opened a new era in multilevel social communication.

For Habermas a language is a factor that arranges the history, funds moral rules and democracy. For Foucault it is a potential medium of control and domination. Habermas, following Kant is a philosopher of a morality grounded on consensus, Foucault deals with a 'real history' which he presents in terms of conflict and power.

Both thinkers belong to postmodernism defined as a cultural era characterised, *inter alia*, by the rise of mass forms of communication, mediazation and commodification of intellectual products and symbolic forms. What differs them is the way of interpretation and understanding the fact that the changes in politics are combined with the changes in technology, especially information and communication technology.

The major achievement of Jürgen Habermas is the development of the original concepts of communicative rationality and discourse theory. He finds rationality in structures of interpersonal linguistic communication. For Habermas the rationalisation of society may be seen in terms of institutionalisation of the potential for communicative rationality.[12]

Coordination of action through language may be achieved when speakers adopt a practical stance oriented toward 'reaching understanding', which, in Habermas' opinion, is a 'inherent telos' of speech. At the end of this process social cooperation would be both deeply consensual and reasonable: actors sincerely agree that their modes of cooperation can be justified as good, right, and free of empirical error. Such a social order depends on the capacity of actors to recognize the intersubjective validity of the different claims on which social cooperation depends. Recognizing the validity of such claims means to resume that good reasons could be given to justify them in the face of criticism.

Relying on these assumptions Habermas constructs the concept of discursive ethics. Its key procedural requirements are as follows. First, (1) no part affected by what is being discussed should be excluded from the discourse, (2) all participants should have equal possibility to present and criticize validity claims in the process of the discourse, (3) participants must be willing and able to empathize with each other's validity claims, (4) existing power differences between participants must be neutralized in such a way that these differences have no effect on the creation of consensus, and (5) participants must openly explain their goals and intentions and in this connection desist from strategic action (in which everyone is oriented toward individual success).[13]

For Habermas the core of the communicative rationality is the unconstrained, unifying, consensus-bringing force of argumentative speech. It is a central experience in life of a human being. The only

12 Habermas (1984–7).
13 Habermas (1993).

force which is active in the ideal speech situation and in communicative rationality is thus this force of the better argument.

The 'discourse' plays the opposite role in the Foucault's work. Large part of it is concerned with power and its relationship to knowledge. He reveals the ubiquitousness of power relations. On Foucault's account, the goals of power and the goals of knowledge cannot be separated: in knowing we control and in controlling we know.

Foucault argues that the 'art of government' represents a continuum between the power we have to govern ourselves, families and environment and the sovereign power of the state.[14] He does not focus on the legitimacy of power but on the essence of power which manifests itself in a 'local or capillary' form. The French philosopher explains how power is created and transferred throughout the 'economy' of discourse and how control over people can be achieved merely by observing them. New centres of power have been identified in professional expertise – e.g. psychiatry, medicine.

At the core of Foucault's picture of modern 'disciplinary' society are three primary techniques of control: hierarchical observation, normalizing judgment, and the examination. The panopticon serves as an ideal architectural model of modern disciplinary power. It is a design so that each inmate is separated from and invisible to all the others in separate 'cells' and each inmate is always visible to a monitor situated in a central tower. Monitors will not in fact always see each inmate; the point is that they could at any time. Since inmates never know whether they are being observed, they must act as if they are always objects of observation.[15]

The principle of the Panopticon may be applied not only to prisons but also to any system of disciplinary power like a factory, a hospital or a school. It pervades every aspect of modern society. It is an instrument through which modern discipline has replaced pre-modern sovereignty as the fundamental power relation. This model of prison is emblematic of a shift towards government through surveillance.

---

14 Foucault (1991).
15 Foucault (1975).

5 Cyberspace: electronic 'lifeworld' or another panoptical project?

Critics often accused Habermas' theory of lack of agreement between ideal and reality, between intentions and their implementation. In abstract terms there is something extremely attractive about his appeal to the force of the better argument as a founding principle of a social order. On the other hand Habermas' vision has being considered as unrealistic and utopian when compared to the actual conditions. Possible cause of this paradox may be sought in a type of technology dominating in a given society.

In the circumstances of modern industrial society the rational potential built into everyday speech is suppressed and to the great extend eliminated by systemic mode of integration. The prime examples of systemic coordination are markets and bureaucracies. In these systemically structured contexts, nonlinguistic media take over the coordinating actions. Hence logic of the system supplants that of the lifeworld.

The burst of a digital revolution brings a technological change. For many people all over the world Internet has become a domain in which consensual modes of action coordination predominate. Using Habermas' terminology it may be called a *sui generis* 'electronic lifeword'.

Some applications of ICT tools surely are an institutionalisation of a potential for communicative rationality. New virtual spaces enable horizontal communication on a massive scale. Various electronic fora, blogs, discussion groups, etc., form a new kind of space where public issues may be discussed and social groups may organize themselves. New forms of co-operation between government and citizens emerge. They have become possible by establishing electronic government services and making public information available on-line.

A good example of a link between new technology and implementation of discourse may be procedures used to generate

Internet Standards. They fulfil the criteria the theory of discourse ethics requires in order to legitimate the rules it produces. The standard-generating procedures of Internet Engineering Task Force exhibit a high degree of self-consciousness and transparency. Electronic communication enables anonymous and pseudonymous speech, which encourages and empowers those unable to afford the time and cost of physical attendance at meetings where Internet Standards are adopted.

Generally speaking, the digital age greatly expands the possibilities for individual participation in the growth and spread of culture, and thus expands the possibilities for the realization of a truly democratic culture based on communicative rationality.[16] Presented examples prove that in the circumstances of informational society a discourse becomes a measure to solve social problems.

Unfortunately it is only half of the truth about the electronic governance. The second face of the god Janus turns toward another aspects of the information technology. Foucault's analysis shows how techniques and institutions, developed for different and often quite innocuous purposes, converged to create the modern system of disciplinary power. Some symptoms the process may be identified in the functioning of an informational society.

Habermas notices that large and complex modern societies can no longer be integrated solely on the basis of shared cultural values and norms. New mechanisms of coordination have emerged, which took the form of nonlinguistic media of money and power. They 'colonize the lifeworld' by displacing communicative forms of solidarity from a social life and inhibiting the reproduction of the lifeworld. It is worth considering to what extend new information technologies may play a similar role.

Because information is an integral part of all human activity, all processes of our existence are shaped by the new technological media. Specific information technologies converge into a highly

16 Balkin (2004).

integrated system. Not only processes are reversible but also organisations and social institutions can be modified and even fundamentally altered by rearranging their technological components, also in a way that enable surveillance and total control.

To put it simply, cyberspace is in its crucial part composed of programs. In this sense code writers may be seen as a *quasi* lawmakers. Their code is able to make the Internet and other electronic media what they desire and regulate what people can and cannot do according to some commercial or political purpose.

The original intent of DRM (digital rights management) was to provide technical means to assure that the artists and publishers can maintain control of their content by restricting use of digital copies in a new environment. Copyright holders using access control technologies are able to limit usage of digital media and devices. Most commonly these technologies find application in film and recordings, online music stores, e-Books and recently in a digital television. Content providers enable users to download and stream an unlimited amount of encoded works on condition they regularly pay subscription fees. When user misses a payment, the service renders all of the downloaded files unusable.

Sometimes digital rights management (DRM) systems restrict use of copyrighted material in ways not included in the statutory law or common law. Certain technologies enable publishers to enforce access policies that not only prevent copyright violations, but also prevent legal fair use. In a common opinion, the presence of DRM also violates some existing private property rights and restricts a range of heretofore normal and legal user activities, like playing legal music on freely chosen player. A DRM component may control a device a user owns by restricting how it may act with regards to certain content, overriding some of the user's actions (for example, preventing the user from burning a copyrighted song to CD). These restrictions usually cannot be disabled or modified by the user. The subject of much controversy is a fact that some variants of DRM software are installed without notification or confirmation and may

include programs which work to subvert control of an operating system from its legitimate operators. Digital rights management technology may be used as a perfect tool of control, that enable not only protection against piracy, but also offer persistent and permanent supervision of the great part of a contemporary intellectual consumption.

The scope of controlling effect of various ICT technologies is not limited to on-line activities and involve people that may do not even know how to use any electronic device. Radio-frequency identification is a popular automatic identification method using devices (RFID tags) which can be stuck on or incorporated usually into a product but also in an animal, or a person. Radio waves are used for the purpose of identifying and reading tags. The method has been so far applied on a massive scale in passports, public transport systems and libraries. In many cases purchasers of tagged items are not aware of the presence of the tag and are not able to remove it. Radio-frequency identification tags affixed to products remain functional for a long time and thus can be used for surveillance and other purposes unrelated to their supply chain inventory functions. Another electronic systems make possible supervision of road traffic, collecting data about routes and drivers.[17]

All mentioned systems work even if there is, metaphorically saying, no one in the guard house. The very fact of general visibility is enough to produce effective social control. Presented examples prove that the panopticon metaphor may be stretched further, beyond the practices mentioned by Foucault (medicine, sex education, psychiatry), and deploy in order to describe the coordination of behaviour taking place in informational society. Its functioning is not necessarily due to the explicit decisions of some central controlling agency. There exist many centres of political, economical and technological power which create their own panoptical projects.

---

17 Reiman (1995).

In addition many ICT tools (e.g. cell phones, PCs with Internet access) are in the same time means of communication for their users and means enabling surveillance of the same users. Explicit answer to the question whether cyberspace is an electronic 'lifeworld' or a panoptical project is difficult. Undoubtedly it has a potential to become each of the two.

6 Prospects for electronic governance systems

Identifying chances and threats connected with the expansion of ICT tools is a first step toward working out a plan of action for the future. Some postulates in the matter of desired shape of electronic governance systems may be outlined at the moment.

It seems obvious that the ICT tools which are fundamental for the functioning the informational society should rely on open source technology. Such a solution will allow for the maintenance and development of the crucial communication architecture. Structural transparency will leave the multitude of end users in control and let them protect their personal autonomy. Only on this condition Internet may remain a real commons that is open to innovation from all comers.

In the field of culture the public domain should be protected in a similar way as the wild nature. It is of great importance not only to the intellectual property system but also to the informational society as a whole. Uncontrollable expansion of intellectual property rights in various areas of information technology disposes others creators of the opportunity to innovate. It is nothing but the public domain that permits the copyright system to work, by leaving the raw material of authorship available for authors to use. The free speech interests are intimately connected to the public domain as well. The increasing-privatization of the public domain weakened the freedom of expression. Freedom of speech and other rights basing on informational process will depend on the design of the technological infrastructure. It may either support the system of free expression and secure widespread democratic participation or not.

Electronic communication is regulated not only by the appellative character of formal and informal rules (normative regulation) but also by electronic constraints. On the Internet, increasingly, rules are enforced not by a human but by a machine. The rules of copyright law, as interpreted by the copyright owner, get built into the technology that delivers copyrighted content. It is code, rather than law, that rules. It works by a digital incorporation of behavioural norms into the architecture of cyberspace. Hence public bodies that take part in electronic governance must be well oriented in the peculiarities of this new mode of regulation.

> In order to develop legal standards of the 'code' one needs to analyse the specific risks of the cyberspace architecture. What specific dangers does the 'code' entails for individual autonomy? How does the code impact on the autonomy of social institutions? And the legal control standards need to be constructed specifically for the architecture of the Internet.[18]

Technical solutions elide the question of power. The technology appears to be 'just the way things are'. Its origins are concealed. Subjects over whom the governance is performed cannot be sure whether its origins lie in state-sponsored scheme or market-structured order. Its effects are obscured because it is hard to imagine the alternative.

As Lawrence Lessig observes the future of copyright law is not so much copyright *law* as copyright *code*. The controls over access to content will not be controls that are ratified by courts; the controls over access to content will be controls that are coded by programmers. And whereas the controls that are built into the law are always to be checked by a judge, the controls that are built into the technology have no similar built-in check. The main task in the process of creation new e-Governance systems is to design it in such a way to enable the control of the governors. The structural differences between 'code' and 'law' must be taken into account as

18 Teubner (2004).

one of the most important issues.[19]

7 Concluding remark

God Janus was a representative of the middle ground between barbarity and civilization, rural country and urban cities, youth and adulthood. He symbolised change and transitions such as the progression of future to past, of one universe to another. There is much to be said for that Janus may patronise today's informational society as well. Ability to reconfigure and change positions is its decisive feature which leads to organisational fluidity. It may easily turn out how much two-faced the conditions of life in such a society are.

In relation to the above issue there is a shift in our understanding of who controls and who is controlled within regimes of technological power that took form of electronic governance. Some features of the digital revolution are conducive to a broad institutionalisation of a discourse as a method of a voluntary co-ordination of behaviour; the others bring us nearer to the vision of a total control done by the inseparable relations of power and knowledge.

These two contradictory visions presented in this article may serve as a philosophical frame for the analysis of the problem of regulation in the digital age. Liberating force of discourse and enslaving effect of the panopticon are two symbolic extreme points, two metaphors between which informational society of the near future will have to find its position.

19 Lessig (2004).

References

Balkin, J. M. (2004), 'Commentary: Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society', *New York University Law Review*, 79.

Balkin, J. M. (1991–2), 'What is a Postmodern Constitutionalism?', *Michigan Law Review*, vol. 90.

Castells, M. (2000), *The Information Age: Economy, Society and Culture. Vol. 1: The Rise of the Network Society*, Oxford: Blackwell.

Foucault, M. (1975), *Discipline and Punish: the Birth of the Prison*, New York: Random House.

Foucault, M. (1991), 'Governmentality', in G. Burchell, C. Gordon and P. Miller (eds.), *The Foucault Effect: Studies in Governmentality*, Wheatsheaf: Hemel Hempstead.

Habermas, J. (1984–7), *The Theory of Communicative Action*, Cambridge: Polity.

Habermas, J. (1993), *Justification and Application: Remarks on Discursive Ethics*, Cambridge, Mass.: MIT Press.

Lessig, L. (2004), *Free Culture*, New York: Free Culture.

MacCormick, N. (1996–7), 'Institutions Normative Order: A Conception of Law', *Cornell Law Review*, vol. 82.

MacCormick, N. (1998–9), 'Institutions and Laws Again', *Texas Law Review*, vol. 77.

Moor, J. H. (1985), 'What is Computer Ethics?', in T. W. Bynum (ed.), *Computer and Ethics*, Oxford: Blackwell.

Reiman, J. (1995), 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future', *Santa Clara Computer and High Technology Law Journal*, vol. 11.

Scott, C. (2005), 'Regulation in the Age of Governance: The Rise of the Post-Regulatory State', in J. Jordana and D. Levi-Faur (eds.), *The Politics of Regulation. Institutions and Regulatory Reforms for the Age of Governance*, Northampton, Mass.: Edward Elgar.

Slaughter, A.-M. (2002–3), 'Global Government Network, Global Information Agencies, and Disaggregated Democracy', *Michigan Journal of International Law*, vol. 24.

Teubner, G. (2004), 'Societal Constitutionalism: Alternatives to the State-centred Constitutional theory?', in C. Joerges, I.-J. Sand and G. Teubner (eds.), *Transnational Governance and Constitutionalism*, Oxford: Hart.

Wilke, H. (1983), 'Der Staat am Verhandlungstisch', in R. Voigt (ed.), *Abschied vom Recht?*, Frankfurt a. M.: Suhrkamp.

CHAPTER 2
TECHNOLOGY

ONTOLOGY-BASED CONTENT MANAGEMENT SYSTEMS IN PUBLIC ADMINISTRATION

Réka Vas,[1] Barna Kovács[2]

1 Introduction

Citizens, businesses and even public administration institutions have to meet challenges provided by the constantly changing business and legal environment. The complexity and quantity of legislation and regulations is increasing at an alarming rate. So research and development projects must turn to the development of innovative, modern technologies enabling citizens and businesses to easily access, understand and apply complex legislation and regulations. Ontology-based content management systems can contribute to the improvement of quality and efficiency of the determinative processes of public administration requiring the application of complex legislation and other legal sources.

Content management systems (CMS) support the creation, management, distribution, publishing, and discovery of corporate information. This definition highly relates to knowledge management and has close ties with the management and presentation of information. So, in contrast with the common opinion content

1 Corvinus University of Budapest, 1093 Budapest, Fővám tér 8., <rvas@informatika.uni-corvinus.hu>.

2 Corvinus University of Budapest, 1093 Budapest, Fővám tér 8., <bkovacs@informatika.uni-corvinus.hu>.

management systems are more than just web content management systems, which are designed to build web and community portals.

Ontology-based content management systems can support further functions, such as semantic enabled search, explication of relations with other documents, drafting of new documents and version management as well. Ontologies, beside the definition of concepts, aim at the most detailed and complete exploration of semantic relations between the concepts of a given domain. Legal sources come in many forms and formats, from different jurisdictions, in different languages, with different internal structures. Ontology-based approach provides support for capturing regularities in a single framework general enough to model the legal content management requirements of multiple jurisdictions. This conception also enables establishing links with legal knowledge systems and legal resources and provides help in maintaining the knowledge base of the CMS as the law changes.

2 Content Management

2.1 What is Content?

2.1.1 *Digital Content*

Providing a precise definition of content is a real challenge. In the literature numerous definitions exist that might subsequently vary according to the authors' focus area. According to Wordnet content has various meanings in different contexts. Content is 'everything included in a collection' and in the context of messages, subject matter and substance, so all that communication is about (Wordnet, 2007). In contrast Wikipedia gives a more adequate definition related to organization life. Accordingly content can refer to

> Information and experiences created by individuals, institutions and technology to benefit audiences in contexts that they value [...] Raw content is in a format that is detectable by an observer [...] Sections, parts or the whole of a document regardless of the medium (Wikipedia, 2007a).

When content is considered in today's computerized organizations, usually digital content is meant under the term. This is a necessary distinction since there are lots of other types of content available in an organization that are on paper or in other various forms that cannot be easily handled by information systems – except when it is digitized.

Information systems deal with the production, processing and retrieving of digital content. The cost of producing digital content is very low compared to the production of any older type of content. This can easily lead to information overload that is a relevant problem of today's information sciences. Accordingly decreasing costs of information creation slightly increases the cost of information processing, mostly in those procedures that require human work.

2.1.2 *Textual Content*

In public administration context content means documents in most of the cases. Documents represent textual data in an unstructured form that makes their processing more difficult. Similarly, there are lots of textual data appearing in an organization that are not documents but can be considered equally important. Communication logs (email or discussion threads) are a good example of such textual data. Currently, other types of content (like audio, video materials or pictures) can be considered less important in an organization, except in cases where they are crucial resources.

Computer programs can easily process textual data – it can be indexed, searched, etc. Processing of non-textual data, in contrast, is a white area on the map of information processing. Currently only humans can describe the content of such data items like videos, audio materials or pictures. These descriptions can be stored as metadata, however producing them requires tremendous work and still not ensures reliable results.

2.1.3 *How does Content Differ from Regular Data?*

As we have seen so far, content and data are related, moreover quite similar terms. Data itself not necessarily has a certain meaning and

usually it is a broader term as content (Skidmore, 2005). However, content is also data itself,[3] to which generally metadata is also assigned (Prideaux, 2005). Content usually has a specific context, name or title and other kinds of metadata associated that can be specified by the Dublin Core standard (Dublin Core Metadata Initiative, 2007) for example. Metadata registered by a telecommunication company on every phone call can be considered as another example.

2.2 Managing Content

2.2.1 *Content Lifecycle*

In the current context content lifecycle can be considered equal to document (e.g. textual content) lifecycle. Document lifecycle usually consists of four major phases: creation, updating, publishing and retiring (Wikipedia, 2007b). So one or more authors create a document that might go through an editorial process of subsequent updates and then it gets published. In this published form it also can be updated several times and finally it gets outdated or retired for some reasons and becomes a subject of archiving or deletion. Content management systems should support these phases in a collaborative manner, since various people can work together on the same content.

Non-textual content can have the same lifecycle pattern, however, it might be more difficult to create or update the content due to the natural characteristics of non-textual data. Also in this case, content management systems should support the whole lifecycle.

2.2.2 *What is a Content Management System?*

The goal of content management is helping the users in creating, organizing, or in other words managing data that is called content in

3 Please consider the system theory view of data-information-knowledge, as presented by Ackoff (1989).

this sense. This also includes the retrieval of information that is one of the greatest challenges for information systems. Retrieving information means the ability of the system to find relevant data for user. If data is found to be relevant relating to the user's problem, then it can be considered as information relevant to user's work. By definition data can be considered as information only when it is relevant in a given context. This is, however, not constrained to information. Retrieved relevant data can also function as knowledge of the individual or the organization when it is used (Ackoff, 1989).

Content is usually handled by Content Management Systems (CMS). Most of the definitions focus on the functionality of these systems, just like the following one:

> system for the creation, modification, archiving and removal of information resources from an organized repository. Includes tools for publishing, format management, revision control, indexing, search and retrieval (Browne and Jermey, [2007]).

2.2.2.1 *CMS vs. WCMS*

The term Content Management System is often confused with Web Content Management System. They share a common root, moreover both are content management systems, but WCMS concentrate on managing content of web portals. CMS are more general in the sense of managing content. So Web Content Management Systems are Content Management Systems with more specific structure and content description formalisms.

2.2.2.2 *CMS Architecture*

CMS usually consist of three major parts: a content creation, a content management and a presentation subsystem, as it can be observed on Figure 1. Content creation part is responsible for managing inputs, in other words gathering content from various knowledge sources. Task of the management part is to store content with appropriate versioning information, ensure access rights management and offer information retrieval functions like full-text search. Presentation part has the role of presenting the content to

different media types like computer screen, mobile devices or printed-paper. This part of CMS has a template engine offering templates for representing content adjusting it to the desired use. Presentation layer also handles user navigation on pages of content – although this function is more relevant in the case of web content management systems.

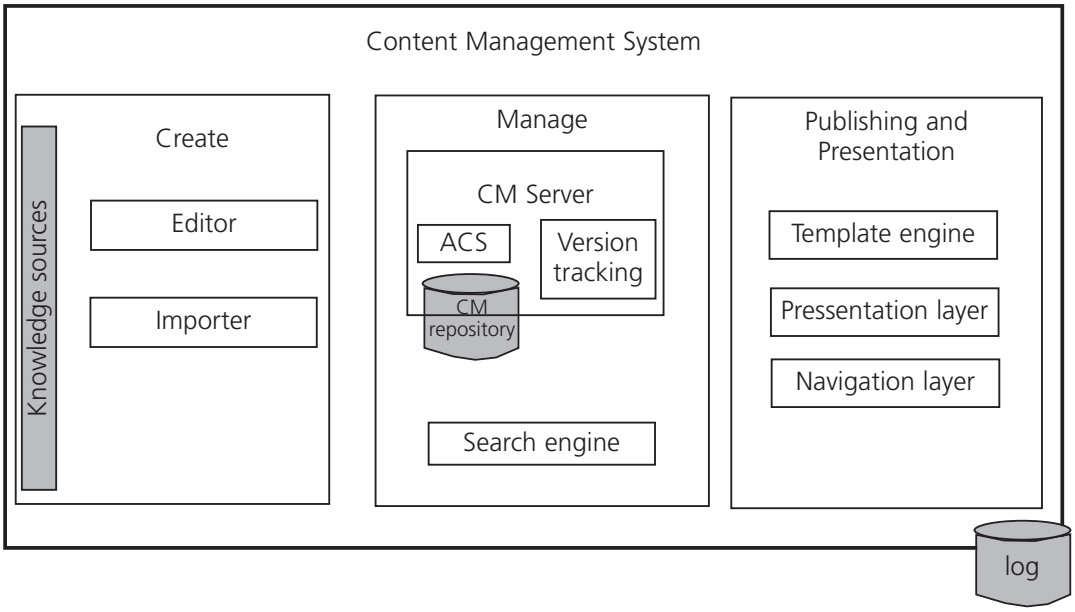

Figure 1. Content Management System Architecture.

2.2.2.3 *Characteristics of CMS*

In an ideal case the role of content management system is to be the nerve center of an enterprise information infrastructure (APQC, 2001: 7). It should aggregate data and information from various sources and deliver to the appropriate recipients. In reality, there are lots of information sources in an organization, but most of them are not directly connected to the content management system. For example laptops of individuals or the heads of employees are not connected to the CMS.

In information system approach content management is more than data management. For managing pure data very sophisticated and

well-developed toolset is available that is called database management system. However DBMS reach their boundaries quite soon in case of processing content. DBMS are mainly managing well-structured data. Content, in contrast, is unstructured with some more-or-less defined metadata descriptors. This requires a completely different approach than data management.

2.2.2.4 *Commoditization*

As a Gartner-study was presenting in 2002, content management is not a standalone product anymore (Caldwell, Gilbert and Hayward, 2002). It is integrated with other enterprise information infrastructure components into larger systems, like Smart Enterprise Suits or corporate portals. Use of CMS is not a competitive advantage anymore, but a necessity. At the same time it is very interesting to see that in the case of content management the reason of commoditization[4] was not the appearance of technology standards but its simplicity. Technology standardization is still under evolution. An example is the JSR-170 standard for Java Content Repository API (Nuescheler, 2005) that describes a standard interface for content management used in Java-based systems.

2.2.3 *Getting the Right Information*

Why is content management so relevant? What is the hidden value in content that made the industry so focused on developing content management systems and then later on developing enterprise applications using content? The answer is simple: it adds further value to corporate assets as a very potent source of knowledge.

Content and knowledge have a strong correlation; they complement and overlap each other in many ways (Kő and Gábor, 2002). Content is a storage of relevant data and information that can be used and reused in a corporate problem context.

The question is how to extract knowledge from the vast amount of stored content. Information overload is a common problem on the

4 Commoditization is the process by which a good becomes a mass product.

field of content management. New content can be created in many different forms, additionally numerous distinct resources can be used for this purpose. These pieces of content can be used and reused many times and this way they become a part of the corporate knowledge body.

On the other hand, already existing knowledge can be codified. In other words knowledge can be expressed in an explicit form and put in the organizational memory as content.

Vast amount of data, information and knowledge is stored as content in a content management system, so the real problem an organization has to face with is how to use them. As mentioned above, decreasing content creation costs cause an increase in the costs of content processing, especially if it requires human work. A solution can be the development of content management systems that provide facilities for effective information retrieval. The keyword is relevance, especially relevance to that business context in which the user is working. The primary challenge in content management is to deliver appropriate content and information to users. Current content management systems provide full-text searching facilities or categorization for enabling the delivery of relevant information. However, still too many results are provided by these solutions, meaning that the applied methods are not distinctive enough.

3 What is an Ontology?

There is no doubt that ontology is a key concept in modern computer sciences. It is also a popular topic in the semantic web community and in the field of developing computer systems that are based on formal ontologies. The wide spectrum of application areas also proves that both business and scientific world has acknowledged that the detailed exploration of semantic relations must stand in the middle of knowledge mapping and processes description – beside the precise definition of concepts. That is what ontologies provide.

Ontologies have long history coming from philosophy. Ontology, as a branch of science theory examining the existent, the being, their principia and characteristics, is part of traditional metaphysics. It is reaching back to ancient Greek philosophy, but the expression has only appeared at the beginning of the XVII century. As Aristotle defined ontology is 'the metaphysical study of the nature of being and existence'.

Much later the term of ontology was picked up by Artificial Intelligence but with a different meaning than in philosophy. On the field of knowledge representation and artificial intelligence many definitions were born for determining the concept of ontology. These definitions have constantly evolved, but despite of this process there isn't any definition that is widely accepted and uniformly used in the community of experts. Instead of providing a comprehensive overview of all existing ontology definitions, it is much more expedient to focus on those definitions that will bring us the closest to the meaning of ontology from a practical point of view. The most quoted ontology definition is linked with the name of Gruber:

> ontology is an explicit specification of conceptualization (Gruber, 1993: 199).

Most researchers generally agree on this definition, but find it too broad. Accordingly Borst amplifies Gruber's definition in the following way:

> ontology is a formal specification of shared conceptualization (Borst, 1997: 12), where
> — formal means that the ontology is machine readable,
> — explicit specification means that concepts, properties, functions, axioms are explicitly defined,
> — shared means that consensual knowledge is stored in the ontology and
> — conceptualization means that an abstract model of some phenomena in the world is formed by the ontology.

In other words ontology is a means to *share information* and to *achieve semantic interoperability* between humans and computers.

Neches and his colleagues take ontology as a tool of knowledge representation:

> ontology defines the basic terms and relations comprising the vocabulary of a topic area as well as the rules for combining terms and relations to define extensions to the vocabulary (Neches et al., 1991: 40).

So according to their approach ontology specifies how to view the world and in which terms we should speak about the world.

Corcho and his colleagues – by taking into consideration several alternative aspects – constructed a rather precise and practical definition of ontology:

> ontologies aim to capture consensual knowledge in a generic and formal way, so that they may be reused and shared across applications (software) and by groups of people. Ontologies are usually built cooperatively by a group of people in different locations (Corcho, Fernández-López and Gómez-Pérez, 2003: 44).

This definition has not altered the basic point, but it includes implications concerning the use of ontology as well that have high priority from a practical point of view. All of the above-mentioned definitions focused on the role of ontologies and said nothing about the structure and components of ontologies. The components of ontology can be briefly stated as:

i) *Classes* – are concepts or tasks of the domain, organized in taxonomies. Concepts (or classes) are general, abstract or concrete notions within a domain of discourse. An ontology is formally describing a domain by describing its concepts (Uschold and King, 1995; Gómez-Pérez, 1999). (E.g.: *student.*)

ii) *Relations* – are 'types of interactions between concepts of the domain' (Gómez-Pérez, 1999) (E.g.: *is-a, subclass-of.*)

iii) *Functions/Attributes* – represent various features and properties of concepts. (E.g.: *student-number.*)

iv) *Axioms/Rules* – Axioms are model sentences that are always true in the given domain. Rules include property restrictions (like cardinality, domain, type).

v) *Instances* – are used to represent specific elements. (E.g.: *Jack is an instance of Student class.*)

These are the most commonly used terms in ontology design.

3.1 How and why do we Use Ontologies?

The primary objective of using ontologies is to solve problems that arise from using different terminology to refer to the same concept or using the same term to refer to different concepts. In order to overcome such problems ontology consists of a set of concepts and a set of constraints determining the way those concepts can be combined. Constraints restrict the number of possible interpretations of concepts, so they impose limitations on the semantics of concepts. At the same time it must be kept in view that in ontologies concepts are represented, not words. Concepts, in general, are not specific of a given natural language.

Uschold defined three main dimensions ((i) Formality, (ii) Purpose, and (iii) Subject Matter) by which ontologies can be classified (Uschold, 1996). From these dimensions we only focus on the purpose dimension that deals with the intended use an ontology may have. Uschold has identified three major application areas, as shown on Figure 2.

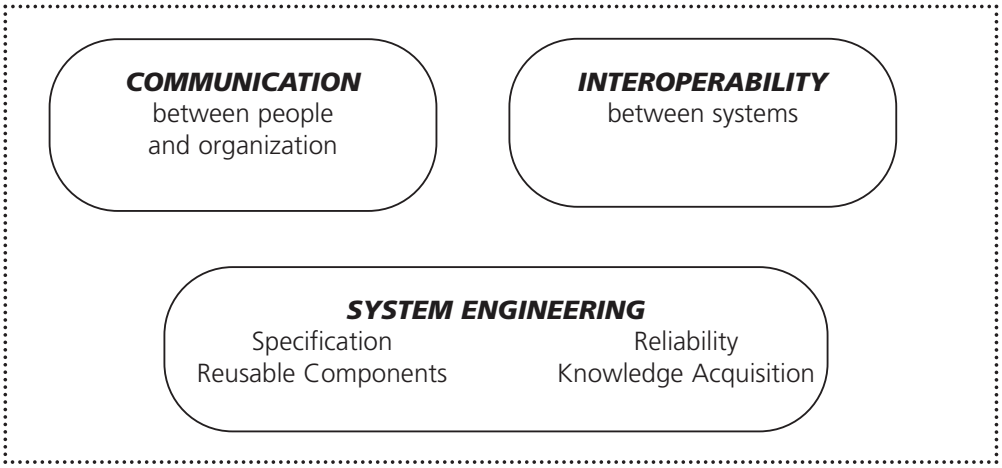

Figure 2. Uses for Ontologies (Uschold, 1996).

Communication ontologies are usually intended for the use among people and not machines. To enable or facilitate communication among people informal and unambiguous ontologies are sufficient. The inter-operability ontologies act as 'interchange formats' (Uschold, 1996) for translations between 'different modeling methods, paradigms, languages and software tools' (Uschold, 1996). The system engineering benefits when using ontology-based development can be summarized as follows (Uschold, 1996):

i) *Re-Usability* – the ontology encodes domain information (including software components) in such way that sharing and reuse are possible.
ii) *Knowledge Acquisition* – the ontology guides knowledge acquisition.
iii) *Reliability* – the ontology 'makes possible the automation of consistency checking resulting in more reliable software' (Uschold, 1996).
iv) *Specification* – 'the ontology can assist the process of identifying requirements and defining specification for an IT system' (Uschold, 1996).

Within the support of communication, interoperability and system engineering an important feature of ontologies is that they make domain knowledge explicit and also enable the reuse and analysis of domain knowledge. However, it must be kept in mind that building an ontology is not a goal in itself.

4 Semantic-Enhanced Content Management

As discussed in previous sections, the main purpose of introducing semantics in content management is to retrieve relevant or the right information. Employing a semantic-enhanced content management system can deliver more appropriate information than the recently used methods of classifying information stored in content. Prerequisite for content management system to become semantic-enabled is to have a domain ontology in the background. This means that the knowledge of a specific domain is processed into a structure representing both the

concepts and the relationships between these concepts. Of course, the larger the ontology is the more content can be described with its help.

4.1 Content Processing in a Semantic-Enabled Content Management System

After formalizing the knowledge of the domain in an ontology, any content that is inserted into the content management system can be annotated with the concepts of the ontology. Concepts can be assigned to the content in general or parts of the content – like in the latter case marking words or phrases in a text for example. This annotation is a formalization of the content, meaning it is a formal description of what is described in the content itself. As soon as it is annotated, not only the usual descriptive metadata (like the metadata specified by the Dublin Core) are known, but through the structure of the ontology the meaning of the content as well. However, it must be stated, that this description relates only to one or some domains – it cannot be assumed that the whole world can be described in a single ontology in finite time. Figure 3 depicts an example of how ontologies and a content management system can be connected.

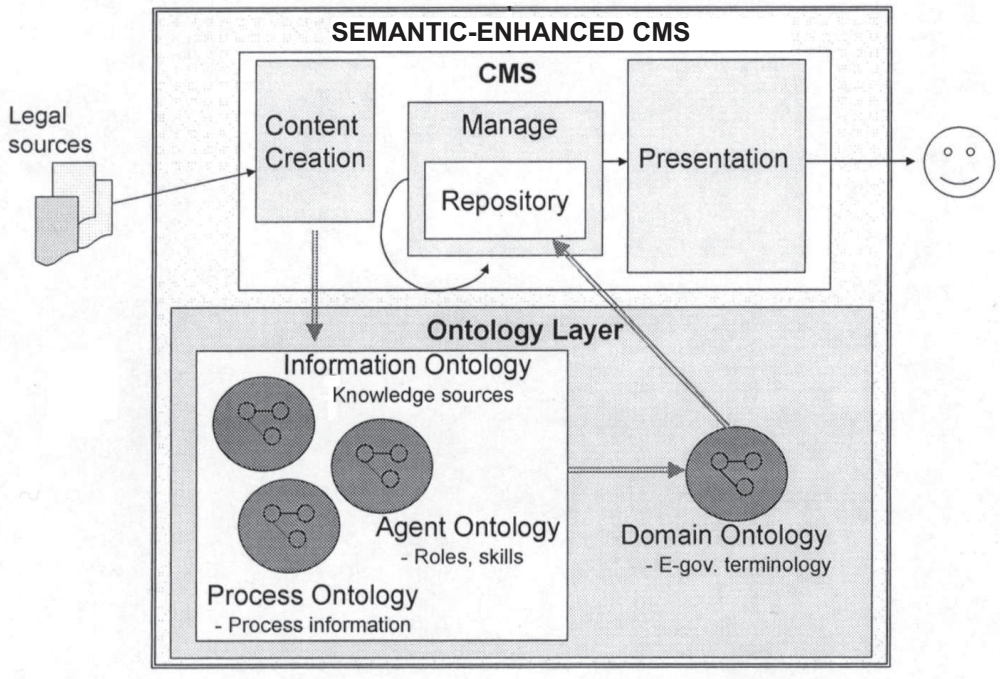

Figure 3. Semantiec-Enhancd Content Management System.

In the next sections the advantages of semantic description of content is compared to classical solutions.

4.1.1 *Semantic-Enabled CMS vs. Document Management Systems*

The role of Document Management Systems (DMS) is to handle textual documents and sometimes other forms of documents. They usually treat these documents as black boxes, using only Dublin Core metadata (like author, title, creation date, etc.) for their description. Generally DMS provide indexing and full-text searching facilities as well. In the semantic-enabled content management approach the domain is represented by an ontology and through this representation the content of a document can be also formalized. This means that the system has a certain knowledge – thanks to all those relations that have already been established between the document and the concepts of the ontology – what the document is about. This information can also be used for inference or searching.

4.1.2 *Semantic-Enabled CMS vs. Full-Text Searching*

Full-text searching uses a word index of content as the source of its queries. Ranking of results is determined by different algorithms based on the frequency of words that are searched. This is one of the most effective approaches of information retrieval used today. However, it has some drawbacks as well. Certain words and expressions may have one or more synonyms. In case of searching for a word that has synonyms it is not ensured that those contents will also be found that only contain the synonyms. Homonyms are problematic as well, since full-text searching cannot distinguish all different meanings of words, making the search results noisy.

Ontology-based content searching means that a concept can be searched independently from its linguistic representation. Actually word forms or expressions are only instances of a certain concept in the ontology. When a concept is looked up, it will be found regardless of its actual appearance.

This feature of semantic-enabled CMS can be easily represented by a simple case from the field of VAT regulation. Natural person, as a concept can appear as customer in VAT regulations. Of course, natural and juristic persons can be customers in the case of VAT as well. When content affecting natural persons are looked up, the VAT law is expected to be found, although the natural person appears using the expression customer there.

4.1.3 *Semantic-Enabled CMS vs. Categorization*

Categorization can be a very good approach to organize and retrieve information. It might have many forms. The most basic approach is single categorization. This is analogous to the folder structure of a hard disk that gives the base of almost every operation system on today's computers. The problem with this approach is that content is organized according to one certain type of logic. It is very hard to find appropriate content if the query follows a different type of logic than the logic of categorization.

Another approach is multiple categorization. This can be done with use of several single terms that is actually nothing else than the very popular tagging. This approach can ensure quite rich content organization, however it can also produce noise in the search results. In this case the categorizing person(s) should think of every possible aspect of search queries to ensure the proper information retrieval. So as a result too many tags are assigned to the content in most of the cases, providing huge amount of search results. If subcategories are used within multiple categorization, such problems will come forward as in the case of single categorization.

In the semantic approach ontology is independent of content. So content is not described by words, but domain concepts (elements of the ontology) are assigned to parts of the content. In case of information retrieval, relationships of ontology concepts can be effectively exploited. For example in the content (a document for example) of request for passport there is no description about natural persons. In the corresponding ontology, however, a relationship between a natural person and a passport is defined, representing that

only a natural person can request passport and passport can only be assigned to a natural person (so both directions can be covered). Even if this relationship is not explicitly defined in any document, according to the domain knowledge formalized in the ontology, the relationship between the natural person and the passport can be discovered and can be exploited.

5 Conclusions

Current development stage of CMS is not sufficient enough to handle that vast amount of information that is created and used in an organization in the course of everyday work. CMS are neither able to effectively manage constantly changing and expanding laws and regulations that are crucial in public administration.

One major problem is the unstructured manner of storing information in CMS. Due to this problem neither the retrieval of information is effective enough. Moreover general information retrieval algorithms (like full-text search or categorization) do not provide relevant enough results.

A solution can be the systematization and formalization of domain knowledge. Ontologies provide a formal representation of the given domain that can be used for mapping the content with the conceptual structure of the domain.

At the same time building an ontology is far from being an easily accomplishable task. So a prerequisite for enabling the use and spread of semantic-enabled technologies is a greater investment of work in the formalization of a domain. As soon as adequate ontologies have been developed they will ease numerous further tasks. So the return on investment is not only realized in the field of information retrieval, but in such other areas like system and application development, communication and in the general operation of the organization.

References

Ackoff, R. L. (1989), 'From Data to Wisdom', *Journal of Applied Systems Analysis*, vol. 16, pp. 3–9.

APQC (2001), *Managing Content and Knowledge*, Report on Survey. ISBN 1-928593-56-9, <http://www.apqc.org/portal/apqc/ksn?paf_gear_id=contentgearhome&paf_dm=full&pageselect=detail&docid=106067> (visited 24 July 2007).

Borst, W. N. (1997), 'Construction of Engineering Ontologies', PhD Thesis, University of Tweenty, Enschede, NL – Centre for Telematica and Information Technology.

Browne, G., and J. Jermey, *Website Indexing – Glossary*, 2nd ed. e-Book <http://www.webindexing.biz/Webbook2Ed/glossary.htm> (visited 24 July 2007).

Caldwell, F., M. Gilbert and S. Hayward (2002), 'CM, Portals and Collaboration Fading: Enter "Smart" Suite', Letter from the Editor, Gartner.

Corcho, O., M. Fernández-López and A. Gómez-Pérez (2003), 'Methodologies, tools and languages for building ontologies. Where is their meeting point?', *Data & Knowledge Engineering*, vol. 46, pp. 41–64.

Dublin Core Metadata Initiative (2007), *ANSI/NISO Z39.85, The Dublin Core Metadata Element Set.* ISBN: 978-1-880124-73-4, <http://www.niso.org/standards/standard_detail.cfm?std_id=725> (visited 24 July 2007).

Gómez-Pérez, A. (1999), 'Ontological Engineering: A State of the Art', *Expert Update*, vol. 2, no. 3, pp. 38–43.

Gruber, T. R. (1993), 'A Translation Approach to Portable Ontology Specifications', *Knowledge Acquisition*, vol. 5, no. 2, pp. 99–220.

Kő, A., and A. Gábor (2002), 'Content Industry and Knowledge Management', in *Proceedings of the 3rd ECKM*.

Neches, R., R. E. Fikes, T. Finin, T. R. Gruber, T. Senator and W. R. Swartout (1991), 'Enabling technology for knowledge sharing', *AI Magazine*, vol. 12, no. 3, pp. 36–56.

Nuescheler, D. (2005), 'JSR 170: Content Repository for Java Technology API', <http://jcp.org/en/jsr/detail?id=170> (visited 24 July 2007).

Prideaux, R. (2005), 'What Does a Content Management System Do?', *TechSoup*, <http://www.icthubknowledgebase.org.uk/whatdoesacmsdo> (visited 24 July 2007).

Skidmore, D. (2005), 'What is the difference between Transactional and Content data in an Internet Packet?', in Mark Warren (ed.), *Fourth Australian Institute of Computer Ethics Conference*, School of Information Systems, Deakin University, Geelong, Victoria (Australia), pp. 51–9.

Uschold, M. (1996), 'Building Ontologies: Towards A Unified Methodology', in *Proceedings of Expert Systems '96, Cambridge, December 16–18th, 1996*.

Uschold, M., and M. King (1995), 'Towards A Methodology for Building Ontologies', in *IJCAI-95. Workshop on Basic Ontological Issues in Knowledge Sharing*, Montreal, Canada.

Wikipedia (2007a), 'Content', <http://en.wikipedia.org/wiki/Content> (visited 24 July 2007).

Wikipedia (2007b), 'Content Management', <http://en.wikipedia.org/wiki/Content_management> (visited 24 July 2007).

Wordnet (2007), 'Content', <http://wordnet.princeton.edu/perl/webwn?s=content> (visited 24 July 2007).

ELECTRONIC MANIPULATION OF EUROPEAN TEXTS ABOUT CONFLICTS OF JURISDICTION: A SEMANTIC WEB TOOL

Mercedes Martínez González,[1] Dámaso Javier Vicente Blanco,[2] Joaquín Adiego Rodríguez,[3] José Manuel Sánchez Felipe,[4] Alma María Pisabarro Marrón[5]

1 Introduction

Legislative databases and public information servers are a common source of information for Law professionals. The legislation these professionals use is great and complex, and querying the European Union public information sources is a laborious task. The project we present deals with the manipulation of Spanish versions of texts of the European Union relative to conflicts of jurisdiction and international assistance on civil matters. The ultimate goal of this project is to obtain an end-user tool for the Association of Representatives on the Court of Valladolid ('Ilustre Colegio de Procuradores de Valladolid').

1 Dpto. de Informática, Universidad de Valladolid, Valladolid (Spain), <mercedes@infor.uva.es>.

2 Dpto. de Derecho Mercantil, Derecho del Trabajo e Internacional Privado, Universidad de Valladolid, Valladolid (Spain), <damaso@der.uva.es>.

3 Dpto. de Informática, Universidad de Valladolid, Valladolid (Spain), <jadiego@infor.uva.es>.

4 Dpto. de Derecho Mercantil, Derecho del Trabajo e Internacional Privado, Universidad de Valladolid, Valladolid (Spain), <jmsf@der.uva.es>.

5 Dpto. de Informática, Universidad de Valladolid, Valladolid (Spain), <alma@infor.uva.es>.

This tools benefits from text mining techniques, which are used to automatically extract from the content of texts structure and other properties that would permit semantic queries (as the Semantic Web community defines this concept) on a collection of legal texts. To facilitate such processes, the organization and articulation of the target texts are tackled. This work is innovative in the use of automatic information extraction applied to these texts; currently, there are no such proposals for texts of this type (EU texts). A collection of XML documents, on which we store the content, structure, and semantic information extracted from texts, is the result of the information extraction processes. In order to permit the querying of this collection the end-user tool will provide user-friendly and personalized interfaces, adapted to the profile of these professionals.

Our work bases on considering the manipulation of structure, references, and metadata, as different, but not isolated, ways of exploiting together documents and relationships. This approach combines information extraction techniques to extract document structure and references (relationships).

The collections used for the experiments with information extraction are Spanish normative texts and normative texts on the international jurisdiction of Community law.[6] User tools mainly work with the last collection, as these are the texts that interest most our end users.

2 Structure extraction

To know the structure of a document has advantages, such as making possible accesses by structure or searching by structure (structured information retrieval). The structure we intend to extract is the one that users recognise during a reading of the document. Normative

6 See Vicente Blanco (2007).

documents are very well-structured documents. They are written as a sequence of divisions, such that each division governs a specific subject-matter within the general matter ruled in the document; each division can itself be subdivided in other divisions in the same manner. Figure 1 shows an example fragment, taken from the Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. The structure is shown on the left, and the content on the right.

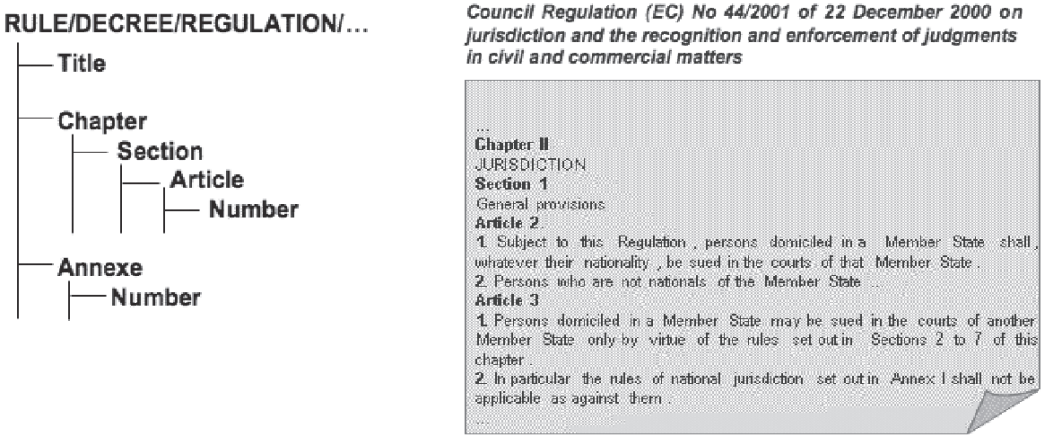

Figure 1. Fragment of a normative document, and its structure.

We take what we consider to be the most natural approach for the extraction: to imitate the method that allows a reader to create a mental image of the said structure while reading the document from start to end. A document part ends where another part begins; the user recognises the start of such parts by the presence of some type of keywords or phrases – pay attention to the fact that it is completely independent of how the document is stored in a digital environment.

The structure extraction is made on document content. It works on digital documents which, if structured, do not present the same structure that is implicit in their content. For example, documents tagged in such a manner that their divisions are not the semantic divisions in which documents creators organized them. These

divisions, which are implicit in document content, are recognised by the presence in text of some expressions that mark the beginning of each division. The process is also a *normalization*: we pass from a document copy whose logical structure does not correspond to the one the users exploit (the implicit structure) to another whose mark-up reflects the semantic implicit structure of the document. The output copy is a XML document. More details of this process can be found in Martínez-González, De la Fuente and Derniame (2003).

The structure extraction was implemented in several steps, and tested on a set of documents containing both Spanish normative texts and EU normative texts. The steps we followed in this process were:

1. The documents were *preprocessed* before taking them as input to the structure extraction process. This phase consisted in transforming to plain text all documents that were not ASCII (Word, for example), pasting a single document from those normative texts that were fragments into several documents, eliminating items we were not interested in (indexes, notes, definitions...), and inserting into plain texts the basic mark-up to mark paragraphs.[7]

At a whole, this preprocessing (that requires a good amount of manual revision) resulted in a set of 1665 well-formed XML documents. We were interested in keeping the tagging at the lowest level (indicating non-standardised, layout dependent divisions, as paragraphs) because it is also used in some references (for example, references as *'In Annex I to..., the eight indent...*'), but the tagging at higher level (the one that should describe semantic divisions) was to be extracted in the next step.

2. The structure extraction process was tested on the document set obtained in the first phase. It functioned with 1583 documents. As this process is implemented on top of a XML parser, it was not able to process documents that kept errors that an XML parser does not

7 This was done with 'lex' and 'yacc', two basic well-known programming tools, which work nicely on layout separations as sequences of blanks and line breaks.

permit: input characters or entities not recognised by the parser ('&icute;', 'º', etc.), tables that were not well-formed and were not corrected during the preprocessing, or documents that did not have a root element.

3 Structured information extraction

Legal documents are intensely related. Besides semantic relationships (documents of the same category, with the same court provenance, etc.), references between documents are frequent. Any document may contain several references to previous rules, jurisprudence, etc., and, in the other direction it can be referenced in many other documents. References are used to include the content of other rules in normative documents (Grupo de Estudios de Técnica Legislativa, 1989), to refer the reader to other documents for further information, or even to modify documents – some normative documents are indeed a collection of amendments to previous normative documents, so that every amendment implies a reference to the modified normative document.

The information to be extracted in this work is mainly of two types: references and metadata. References are pieces of text that serve to refer to other document (or part of a document). Metadata is data about the documents that can be also extracted from its content; in our case, the participant states of a document. We focus in the following on the reference extraction.

References to normative documents are in many cases references to internal fragments. The position of fragments with respect to the internal structure of the document is used to identify them. This is applicable both to internal references (references to the same document) and to external references (references to other documents). The reference extraction process is based on an analysis of document content. Its main steps are described in Martínez-González and De la Fuente (2007) and they are summarised

hereafter. Four steps are needed. The first one is an analysis that permits to discover the structure rules exploited in references. Next, it is necessary to identify how this structure is used in references. This is the second step. After this, the method that permits to extract references from document content can be designed. Part 3.1 describes this third step. Finally, the references detected are resolved. This is the fourth step. For this task an algorithm was devised and implemented. Its details are presented in Martínez-González and De la Fuente (2007).

3.1 The taxonomy that supports the reference extraction

The extraction of references consists in an analysis of document content. The references extraction is based on a set of grammars, which themselves are related with a taxonomy of references. This taxonomy considers four criteria:

1. The *type* of item referenced: there are references to documents, or to fragments of documents. First row of Table 1 shows an example of a reference to a 'document', while in the second row a 'fragment' is referenced.

2. The *range* of the reference: internal references refer to the same document in which they are, while external references, like the one in first row of Table 1, refer to other documents.

3. The *number* of units referenced: a simple reference concerns a single referent, as it happens in the example in first row of Table 1. In a multiple reference, several items are targeted simultaneously.

4. The use of *context* information need to solve the reference: to solve relative references, some context information (documents referenced before, close to the current reference, in a specific part of the same document...) is needed. However, to solve direct references, as those in rows 1 and 2 of Table 1, no context information is necessary.

Any reference can be classified on all of these four criteria. Table 1 shows some examples of references and their classification.

Reference	*Type of item*	*Range*	*Number of units*	*Context*
Council Decision 1998/468/EC of 28 June 1999	Document	External	Simple	Direct
Articles 68 and 72 to 74 of the Code of Civil Procedure	Fragments	External	Multiple	Direct
Without prejudice to Article 4	Fragment	Internal	Simple	Relative
The Treaty and the Conventions referred to in Article 69	Document	External	Multiple	Relative

Table 1. Some example references and their classification, according to the taxonomy of references presented in section 3.

4 XML in the implementation

The adoption of XML to model legal documents is getting so general, that we can state that it is *the* language for legal documents. Several schemas have been created for this goal (Arnold-Moore, 2000; Boer, Van Engers and Winkels, 2002; Bolioli et al., 2002; Finke, 1997; Marchetti et al., 2002; Martínez-González, De la Fuente and Derniame, 2003; Palmirani and Brighi, 2002; Sjöberg, 1997a, 1997b) and more keep being produced. At the same time, the manipulation of structure is an inherent property of XML, which facilitates the implementation of processes that exploit the structure of documents.

We have used XML to store documents and the associated data. Documents and data have corresponding schemas, represented in XML as DTD or XML schemas, so that these data can be validated by using an XML parser. Besides, we take profit of XSLT, the XML Stylesheet Transformation Language (Clark, 1999) and XPath (Clark and DeRose, 1999).

5 User tools

There are several user tools built in order to facilitate the use of the information extraction tools by users, to facilitate the supervision of

the results, or to permit to end-users to access documents and their information. At present, the tools that are already built permit:

1. To navigate documents, using their structure or the hypertext network built from links that represent references (see in Martínez-González, De la Fuente and Derniame, 2003, more details about this). This tool offers a web interface. The HTML documents are built automatically from the XML data stored using XSLT, the XML Stylesheet Language Transformation. Figure 2 shows a snapshot of this tool.

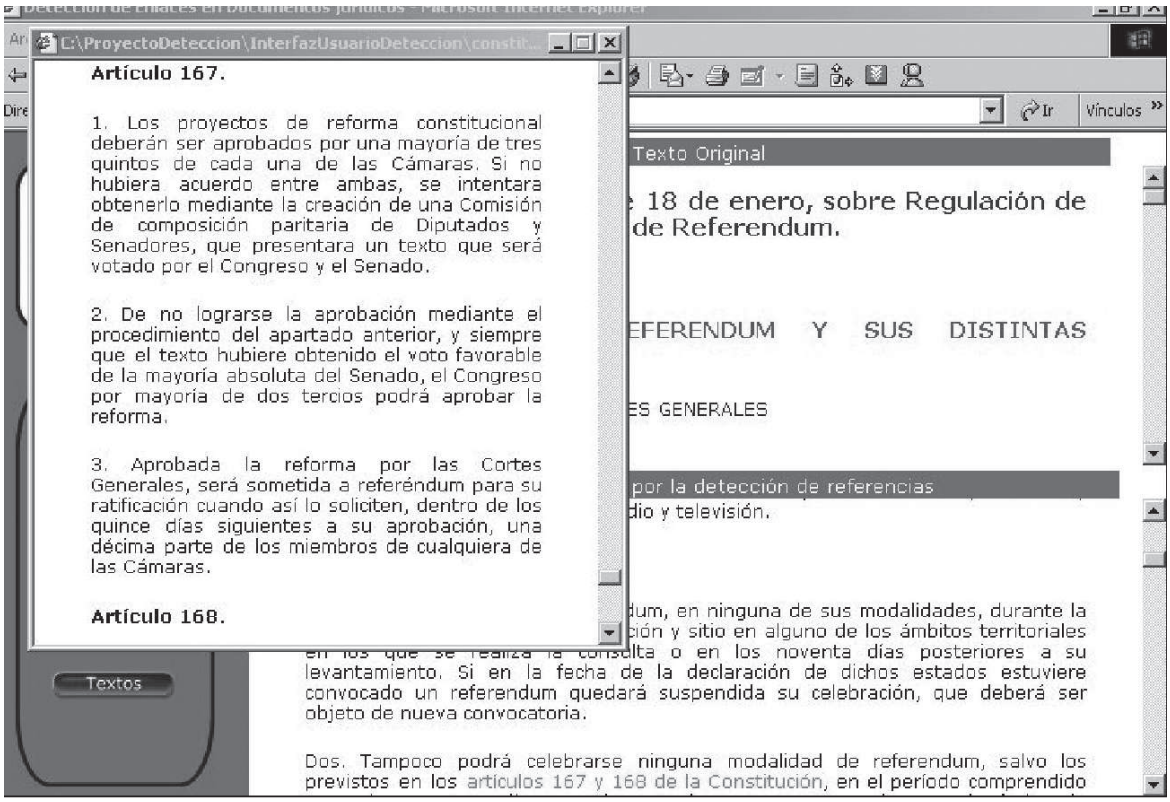

Figure 2. A web tool to navigate documents and references.

2. To revise the references extracted automatically. If necessary the data that describes each reference can be modified. As well, the tool permits the manual insertion and deletion of references that have not been correctly detected by the reference extraction processes. This

tool is conceived to facilitate the work of experts in the reference extraction. It is worth noting that this is a profile different than the one of users of tools described in items 1 and 3, which are jurists. A snapshot of this tool is shown in Figure 3.

3. To access the collection of EU documents about conflicts of jurisdiction. There are two versions of this tool. The first one permits to its user to work autonomously with its own collections and data. In the second one there is a central server that maintains the collections and associated data. This one has been used in some teaching practice case, presented in Vicente Blanco et al. (2007). Figure 4 shows a snapshot of this tool.

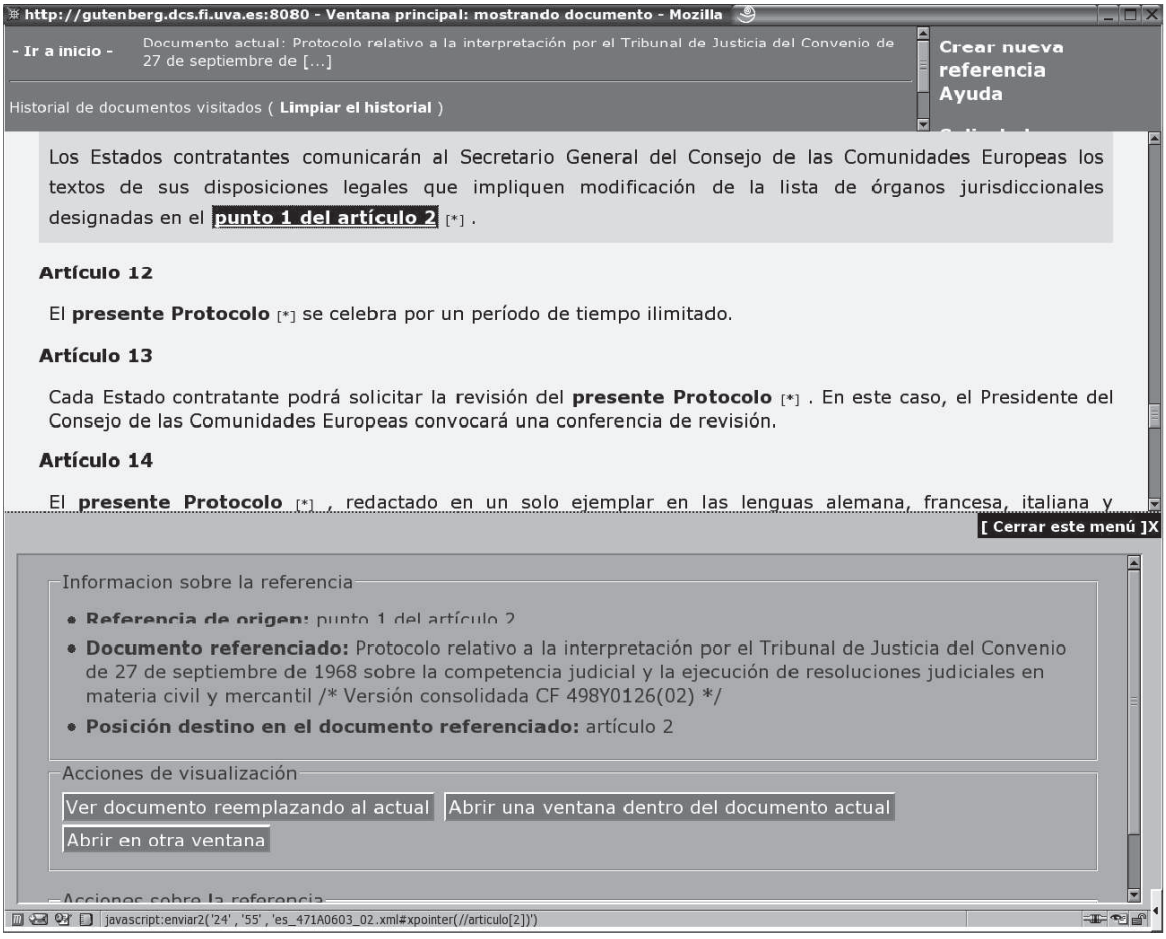

Figure 3. A tool for the revision of results from automatic reference extraction.

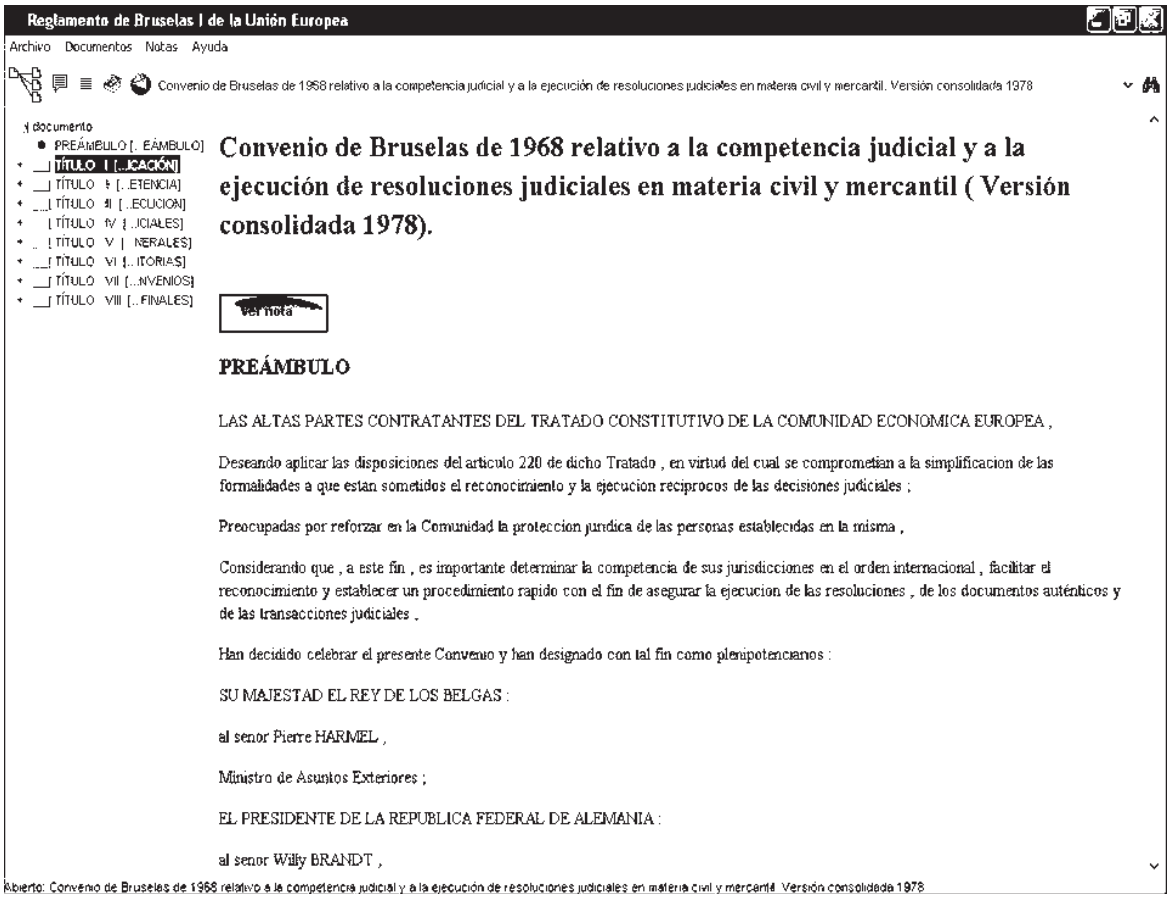

Figure 4. A tool that permits to handle documents and annotations.

6 Conclusions

The work presented in this paper deals with the manipulation of Spanish versions of legal texts. Its main technical characteristics have been presented briefly and the references to some publications that extend the details have been included. In addition, the user tools developed or under development have also been presented.

The current work focuses on tools for the Association of Representatives on the Court of Valladolid ('Ilustre Colegio de Procuradores de Valladolid'), which is a goal of the research project that supports part of this work. This tool started from a web version of the tool used in the e-Learning experiences described in Vicente Blanco et al. (2007). However, it includes additional functionality, within which we remark

the possibility of document comparison (see a snapshot of its current state in Figure 5) and concept-based search. The software that implements the concept-based search is currently under development. It takes profit from the results obtained by this team with indexing in information retrieval (Adiego, Navarro and De la Fuente, 2007). Thesaurus will support the substitution of *term search* by *concept search*.

Future work includes the development of an update service. It will permit autonomous user applications to update local collections, under user requirement, with new documents. This update service will be implemented on top of web services. Besides, we are currently on the process of selecting some jurisprudence related with the normative documents we already have. These documents will be inserted as a new collection in the corresponding databases.

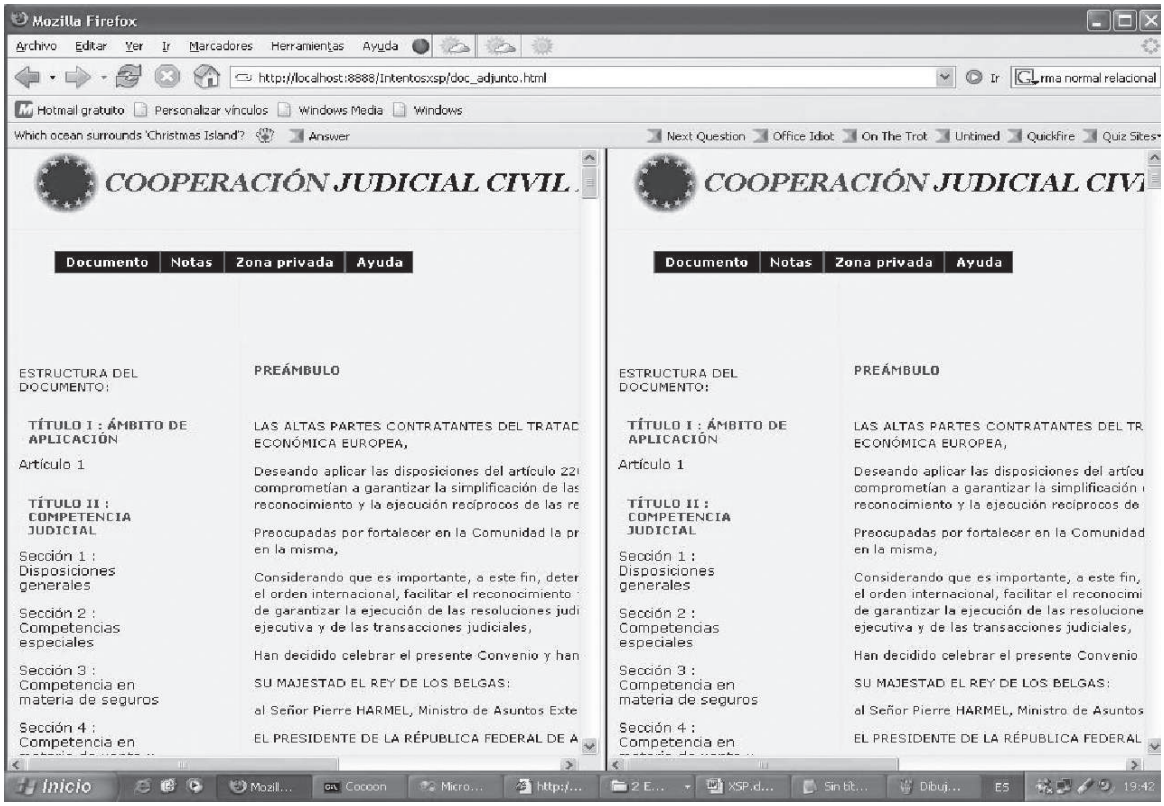

Figure 5. A comparison of documents in the new prototype of the end-user web tool.

Acknowledgements

The implementation of reference extraction was carried out by Sandra Muñoz Mínguez, Nuria Serrano and Yoana Martín. The reference revision interface was implemented by Jesús Requejo. The web version of the end-user tool is being implemented by Matías del Hoyo and Pablo Encinar. Víctor Manuel Merayo implemented the prototype used in the e-Learning experience. All of them are students at the University of Valladolid (Spain).

References

Adiego, J., G. Navarro and P. de la Fuente (2007), 'Using Structural Context to Compress Semistructured Text Collections', *Information Processing and Management*, vol. 43, no. 3 (May), pp. 769–90.

Arnold-Moore, T. (2000), 'Connected to the law: Tasmanian legislation using EnAct', *Journal of Information, Law and Technology*, 1.

Boer, A., T. van Engers and R. Winkels (2002), 'Proposal for a Dutch legal XML standard', *Lecture Notes in Computer Science (LNCS)*, vol. 2456, pp. 142–9.

Bolioli, A., L. Dini, P. Mercatali and F. Romano (2002), 'For the automated mark-up of Italian legislative texts in XML', in T. Bench-Capon, A. Daskalopulu and R. Winkels (eds.), *Legal knowledge and information systems. JURIX 2002: 15th annual conference, December, 2002, Proceedings*, Amsterdam, Netherlands, London, UK: IOS Press, pp. 21–30.

Clark, J. (1999), 'XSL Transformations (XSLT) Version 1.0', *W3C Recommendation 16 November 1999, W3C, the World Wide Web Consortium*, <http://www.w3.org/TR/1999/rec-xslt-19991116>.

Clark, J., and S. DeRose (1999), 'XML Path Language (XPath) version 1.0', *W3C Recommendation 16 November 1999, W3C, the World Wide Web Consortium*, <http://www.w3.org/TR/1999/xpath>.

Finke, N. (1997), 'TEI extensions for legal texts', in *Text encoding initiative tenth anniversary user conference*, Providence, RI, USA.

Grupo de Estudios de Técnica Legislativa (1989), *Curso de técnica legislativa GRETEL. Serie de Técnica Legislativa I*, Madrid: Centro de Estudios Constitucionales.

Marchetti, A., F. Megale, E. Seta and F. Vitali (2002), 'Using XML as a means to access legislative documents: Italian and foreign experiences', *ACM SIGAPP Applied Computing Review*, vol. 10, no. 1, pp. 54–62.

Martínez-González, M., and P. de la Fuente (2007), 'Introducing structure management in automatic reference resolution: An XML-based approach', *Information Processing and Management*, <doi:10.1016/j.ipm.2006.12.004> [in press].

Martínez-González, M., P. de la Fuente and J.-C. Derniame (2003), 'XML as a means to support information extraction from legal documents', *International Journal of Computer Systems, Science and Engineering*, vol. 18, no. 5, pp. 263–77.

Martínez-González, M., P. de la Fuente and D. J. Vicente Blanco (2004), 'Dealing with the automatic extraction of references from legislative digital libraries', in *VSST 2004 (Veille Strategique, Scientifique et Technologique)*, pp. 281–8.

Martínez-González, M., P. de la Fuente and D. J. Vicente Blanco (2005), 'Reference Extraction and Resolution for Legal Texts', *Lecture Notes in Computer Sciences (LNCS)*, vol. 3776, pp. 218–21.

Martínez-González, M., P. de la Fuente, J.-C. Derniame and A. Pedrero (2001), 'Relationship-Based Dynamic Versioning of Evolving Legal Documents', *INAP (LNCS)*, vol. 2543, pp. 290–305.

Palmirani, M., and R. Brighi (2002), 'An XML approach for Italian legislation acts', in Institute of Advanced Legal Studies, *JURIX 2002 workshop on e-Government*, London, UK.

Sjöberg, C. M. (1997a), 'Corpus legis: a legal document management project', *International Journal of Law and Information Technology*, vol. 5, no. 1, pp. 83–99.

Sjöberg, C. M. (1997b), 'DTD development for the legal domain', in *SGML Sweden'97*, Stockholm, Sweden.

Vicente Blanco, D. J. (2007), 'Medios electrónicos de pago y jurisdicción competente en supuestos de contratos trans-fronterizos en Europa. Los criterios de competencia judicial del

Derecho comunitario europeo y su aplicación a las relaciones contractuales involucradas en los medios electrónicos de pago', in R. Mata Martín (ed.), *Los medios electrónicos de pago. Problemas jurídicos*, Granada: Comares, pp. 269–318.

Vicente Blanco, D. J., M. Martínez-González, J. M. Sánchez-Felipe and J. M. Adiego Rodríguez (2007), 'Experiences on teaching International Private Law with the support of an e-Learning tool', in *The LEFIS Virtual Campus design, Albarracín Meeting, 18th–19th May 2007*, <http://www.lefis.org/meetings/workshops/2007/albarracin_2007/index.htm> (visited 27 July 2007).

THE USE OF ALPHABETS OTHER THAN LATIN (ROMAN) ON THE INTERNET AND ITS IMPACT ON BUILDING A TRUE KNOWLEDGE SOCIETY

Oleksandr Pastukhov[1]

1 Introduction

The days when the English language dominated the global Internet scene are long gone. According to Global Reach, a company active in global online marketing, multilingual Web promotion and Website translation that has been tracking linguistic communities online since 1995, the non-English-speaking online population's share reached 64.8% of the global Internet audience by September of 2004.[2] The online presence of the United States, the cradle of the Internet, the e-Commerce leader and trendsetter, is steadily shrinking. According to comScore Networks, a Chicago-based market research firm, around 14% of the 694 million Internet users worldwide in March 2006 were in the US (down from about 2/3 a decade ago), while 25% of the world's 'wired' population came from China, Japan, India and South Korea.[3] But this is not all! Some 45 million people out of the total of around 255 billion people living in the US itself identified

---

1 Center for the Law of ICT (CLICT), 39 Shesti Septemvri St., Sofia 1000, Bulgaria, <alex.pastukhov@clict.net>.

2 See <http://www.global-reach.biz/globstats/index.php3>.

3 See Victoria Shannon, 'More world on the Web', *International Herald Tribune*, 11 May 2006, p. 16.

themselves as not speaking English at home at the 2000 census.[4] What is more, SIL International estimates that 38% or 7.7 million households in the United States are headed by immigrants.[5]

It is logical to conclude that all these people whose mother tongue is not English are prone to access non-English Web resources and can be better served on the Internet in their own language. No wonder the online content has been quick in responding to this new reality: only 56.4% of all Websites were in English in 2002.[6]

Yet a content in a native language is obviously not enough. To navigate the Web with ease and confidence, its users need reference points that are meaningful to them and that they can rely on. The best such points on the Internet are domain names, addresses at which Websites are located. Naturally, to be easily recognized and memorized by the travellers through the Net, domain names have to be in their native language, too.

Internet entrepreneurs are equally interested in domain names – powerful marketing tools – being in national languages, for they realize that '[t]echniques such as index registrations, optimization of home pages for foreign keywords, online promotion, strategic linking, PR, affiliate programs, direct email and banner advertising are all excellent in order to build traffic to a multilingual Website... as long as each technique is performed in the language of the target markets' [hyperlinks omitted].[7] And the potential non-English-speaking online clientele is growing exponentially. Thus, the number of Chinese-speaking people having Internet access grew fourfold in the five years before 2005.[8] Maybe learning foreign languages has

---

4 See <http://www.factfinder.census.gov/servlet/DTTable?_bm=y&-geo-id=D&-ds_name=D&-_lang=en&-mt_name=ACS_C2SS_EST_G2000_P034>.

5 See *Languages of USA*, <http://www.ethnologue.com/show_country.asp?name=US>.

6 See <http://www.netz-tipp.de/languages.html>.

7 <http://www.global-reach.biz>.

8 See 'Language diversity to continue net's rise as No. 1 communication medium', *The Sydney Morning Herald*, 11 April 2006, available at <http://www.smh.com.au/news/perspectives/language-diversity-to-continue-nets-rise-as-no-1-communicationmedium/2006/04/10/1144521238556.html>.

not become particularly fashionable in Asia yet, but many people in that part of the world can already afford buying things over the Internet. In the Internet-savvy South Korea,[9] for instance, B2C transactions amounted to $6.3 billion in 2004.[10]

2 Technological solution

All the above being said, the Internet is in obvious need for an address system relevant and effective for different linguistic groups to become a vital and truly global tool for commerce, government and learning. Yet while domain names in languages using Latin (Roman) alphabet (or, in the IT specialists' vernacular, script) present no problem from the addressing technology standpoint, although no diacritical marks are envisaged in the standard ASCII[11] 28-letter encoded character set,[12] domain names in languages using other alphabets involve a number of technological problems. The first step in their solution was made in 1998, when a Swiss researcher proposed a way to encode non-English equivalents of the generic suffixes .com, .org and .net. Soon afterwards, Dr. Tan Tin Wee, a biochemist at the National University of Singapore, being concerned by the East-West digital divide, set out to test and developed the idea.

---

9 See, e.g., *Economies by broadband penetration*, 2005, at <http://www.itu.int/ITU-D/ict/statistics/at_glance/top20_broad_2005.html>.

10 See e-Marketer, *Asia-Pacific e-Commerce: Spotlight on China, Japan and South Korea*, 1 July 2005, abstract available at <http://www.marketresearch.com/product/display.asp?productid=1118411&xs=r&SID=92533116-353343214-277637010&curr=USD&kw=&view=abs>.

11 ASCII stands for American Standard Code for Information Interchange, a coding method that defines 128 characters, including alpha characters, numbers and punctuation marks. For more detail, see Harry Newton, *Newton's Telecom Dictionary*, 19th ed., CMP Books, 2003, p. 73.

12 See Jonathan Wright, 'Fully Arabized Internet has some way to go', *Reuters*, 26 May 2004, available at <http://www.minc.org/MINCinPRES/Reuters%20%20Latest%20Financial%20News%20-%20Full%20News%20Coverage.htm>. ('Even the humble umlaut, the two dots written over German vowels, is a recent addition to the domain name system, confined so far to registries of names run by German-speaking countries.')

Later in 1998, he shared the early versions of the technology with the Japanese, Chinese, Taiwanese and Korean network information centers (NIC), national bodies that administer country-code top-level domains (ccTLD) such as .jp for Japan.[13]

Initially rejected, the technology was later appropriated by the Chinese and Taiwanese NIC to be used in their respective domain zones. Korean and Japanese NIC entered the fray thereafter and registrars from outside the region such as American Network Solutions or Australian Melbourne IT followed the suit over the fear of loosing the Asian domains market to local competition.[14]

The array of standards utilizing different downloadable plugin software resulted in confusion by customers who could not always find Websites they wanted and the necessity for businesses to register the same domain name with several registrars.[15] Conflicting registrations of virtually identical domain names in China and Japan were also reported.[16] The situation clearly called for a uniform solution.

The task of finding a common ground was vested in the Multilingual Internet Names Consortium (MINC), a non-profit non-governmental organization formed in June 2000 to promote the internationalisation of Internet names, including domain names.[17] In the multilingual domains realm, the Internet standards community

---

13 See Kathy Wilhelm, 'Tongue-Tied on The Net: The race to grab a piece of the potentially lucrative market in Asian-language domain names threatens the future of a multilingual Web that works', *Far Eastern Economic Review*, 22 Feb. 2001, available at <http://www.minc.org/pr/feer2001.shtml>.

14 See Kristie Lu Stout, 'Asia's multilingual mess on the Net', *CNN.com*, 19 Feb. 2001, available at <http://edition.cnn.com/2001/WORLD/asiapcf/southeast/02/18/sing.multinet/index.html>.

15 See supra footnote 13.

16 See, e.g., Kabushiki Kaisha Sangyokeizai Shimbunsha v. Jg Kim (WIPO Case No. D2001-0620), available at <http://arbiter.wipo.int/domains/decisions/html/2001/d2001-0620.html>.

17 See <http://www.minc.org>. For MINC membership, see Press Release, 'Formation of MINC, the new Multilingual Internet Names Consortium, draws founding membership from key Internet organisations and industry leaders', Yokohama, 19 July 2000, at <http://www.minc.org/pr/foundingmemberJul2000.shtml>.

found itself playing catch-up. Such organizations as the Internet Engineering Task Force (IETF), a subdivision of the Internet Activities Board (IAB), and the Internet Corporation for Assigned Names and Numbers (ICANN) have united their efforts to study the competing standards and to propose a single one that would not lead to fragmentation of the Internet and safeguard its seamless operation. Their cooperation with VeriSign, the registry for .com and .net generic top level domains (gTLD), made registering names using non-ASCII characters with .com and .net suffixes possible since November 2000, when VeriSign started its Internationalized Domain Name (IDN) Testbed.[18] Currently, VeriSign offers registration of IDN in 32 scripts covering 350 languages.[19] The company also contributed significantly to the IETF's work on IDN standards that were published in December 2002 and March 2003 as four requests for comment (RFC). [20]

3 Regional developments

The Cyrillic alphabet, created by St. Cyril and Methodius in the 9th century and subsequently developed by St. Clement of Ohrid in the Middle Ages, is currently in use by more than 50 European and Asian languages.[21] The Internet community in the part of the world where Cyrillic alphabet is used have been very enthusiastic about the IDN technology from the outset. The most proactive registrars have started registering domain names in Cyrillic from the moment it became technologically feasible. The Russian RegTime.net Limited

---

18 See <http://www.verisign.com/products-services/naming-and-directory-services/naming-services/internationalized-domain-names/idn-standards/verisign-idn-testbed/index.html>.

19 See <http://www.verisign.com/products-services/naming-and-directory-services/naming-services/internationalized-domain-names/page_001382.html>.

20 See <http://www.verisign.com/products-services/naming-and-directory-services/naming-services/internationalized-domain-names/idn-standards/idn-standards-summary/page_002202.html>.

21 See Bulgarian alphabet, at <http://www.kirildouhalov.net/language/ alphabet.html>. Cyrillic alphabet, at <http://www.omniglot.com/writing/cyrillic.htm>.

became the pioneer on May 22, 2001, long before IDN were officially accorded their own standards, when it launched its all-Russian domain name registration service allowing registration of gTLD with .ком, .нет and .орг (analogues of .com, .net and .org, respectively) suffixes.[22] The service became possible through a registrar partnership with i-DNS.net International, a National University's of Singapore spin-off initiated by Dr. Tan Tin Wee back in 1999.[23]

On April 30, 2003, .ком, .нет and .орг were approved by MINC as common gTLD in Bulgarian, Russian and Ukrainian, whereas .бг, .ру, and .ya became territorial TLD for Bulgaria, Russia and Ukraine, respectively.[24] On May 25, 2003, the Draft Internationalized Domain Names Registration and Administration Guideline for Russian, Ukrainian, Bulgarian and Byelorussian languages[25] was published by Cyrillic Languages Internet Names Consortium (CyrLINC), an organization established to coordinate efforts to develop the IDN system and applications within countries and territories using Cyrillic alphabet.[26]

On June 11, 2003, registration of domain names with the .ру suffix for the first time became possible at the RegTime.net's Webnames.ru portal.[27] The price of registering a name in Cyrillic zones remains relatively high since then, whereas a 'special offer' section of the site features registration of 'top-domains' such as бизнек.ру (business.ru) or 'super-domains' such as банк.ру (bank.ru) for $999 and $4999, respectively.[28] Yet higher prices do not seem to be deterring Russian

---

22 See <http://www.regtime.net/en/index.pl>.

23 See 'National University of Singapore Announces the Launch of the Home-Grown High-Tech Internet Company, i-DNS.net, Pioneer of the Global Multilingual Domain Name System', at <http://www.i-dns.net/newsroom/news/I-SG991101-01.html>.

24 See <http://www.webnames.ru/en/scripts/news.pl under 05.05.2003>.

25 See <http://www.cyrlinc.org/docs/draft-cyrlinc-idn-reg-00.txt>.

26 See <http://www.cyrlinc.org>.

27 See <http://www.webnames.ru/en/scripts/news.pl>, under 11 June 2003.

28 See <http://www.webnames.ru/en/services.pl>.

businesses, more than 30% of which had been using the .ру suffix as an element of their pictorial and textual trademarks even before registering a corresponding domain name became reality.[29] The secondary market for domain names in Russian appeared immediately: many 'catchy' names are offered for sale at the same site.[30] Surprisingly, интернет.ком (internet.com) was offered for $2 at the time of writing.

In the author's native Ukraine, the country's territorial Cyrillic domain .ya was expected to take off by the end of 2004,[31] but never did because of the events that got to be known as the Orange Revolution and the political turmoil of the following year. The registry, as well as the registry for the .бг zone, is still to be determined by the MINC on a competitive basis, whereas CyrLINC has been already named the .ру registry.[32]

On the other side of the world, in China, meanwhile, the availability of government-approved domain names completely in Chinese characters has been announced.[33] The domain names are available under the top-level Simplified Chinese character extensions 'gongsi' ('company') and 'wangluo' ('networking'). Even the 'dot' character can be typed in either ASCII or Chinese character. Registrants of names in Simplified Chinese characters will get a corresponding name in Traditional Chinese characters used in Hong Kong and Taiwan. A new generic extension '.zhongguo' ('.china') along with Chinese keywords were also approved, but only in the Simplified Chinese script for now.[34] Almost immediately thereafter, the

---

29 See supra footnote 26.

30 See <http://www.webnames.ru/en/scripts/selldomlist.pl>.

31 See <http://itt.com.ua/4098>.

32 See <http://www.webnames.ru/en/scripts/news.pl>, under 13 May 2003.

33 See 'The Ministry of Information Industry of the People's Republic of China Endorses Internet Domain Names Completely in Chinese Characters at the 14th Internet in China Conference', at <http://www.i-dns.net/newsroom/news/OL040907-01.html.en>.

34 See 'New China-Government Approved Chinese character Internet domain names, widely usable in China, available for registration', at <http://www.i-dns.net/newsroom/news/GE041001-01.html.en>.

mainland China's NIC – CNNIC – reported its resuming of control over domain names containing names of Chinese Olympians registered in bad faith.[35] Already some major global brandnames like L'Oreal and BMW have run into some 'trouble' with cybersquatting in the Chinese-speaking sector of the Internet.[36]

This brings us to the question of the interrelation between designations in the 'real' world and names in the 'virtual' space. The most economically significant of the former are, of course, trade names and trade or service marks (hereinafter collectively referred to as 'trademarks' or simply 'marks'). Trademarks are a 'breed' of intellectual property with an utmost significance for the Internet. Domain names which do not contain trademarks but comprise such 'catchy' words as 'money', 'casino', 'credit', 'travel' or 'tickets' can also prove useful for businesses, no matter where or in which language they are registered.

At the same time, the most widely accepted mechanism for the adjudication of Internet names – the ICANN's UDRP – and variations thereof are currently applicable only to disputes over domain names containing trademarks (trade names, personal names and geographical indications are excluded) and only to domain names registered by ICANN-accredited registries of 10 gTLD (including the .com and .net IDN registered under the VeriSign IDN Testbed)[37] and 44 (including .io) ccTLD.[38] 'Among the other current, or planned, internationalized domain name solution providers, there is no uniformity of application of the UDRP, or any adaptation of it, so as to ensure protection for intellectual property holders or a uniform system of dispute resolution across the gTLD

---

35 See 'CNNIC Regains Chinese Domain Names of Chinese Olympians from Cybersquatters', at <http://www.i-dns.net/newsroom/news/OL040907-01.html.en>.

36 See 'New China-Government Approved Chinese character Internet domain names, widely usable in China, available for registration', at <http://www.i-dns.net/newsroom/news/GE041001-01.html.en>.

37 See <http://arbiter.wipo.int/domains/gtld/udrp/index.html>.

38 See <http://arbiter.wipo.int/domains/cctld/index.html>.

space'.[39] Thus, CNNIC, the government-appointed registry of .cn and all-Chinese domain names,[40] has adopted its own Domain Name Dispute Resolution Policy and the Rules implementing it.[41] Furthermore, according to the China Internet Domain Name Regulations introduced by the Order No. 24 of the Ministry of Information Industry of the People's Republic of China, '[i]f the decision of the domain name dispute resolution institution is in conflict with the legally effective judgment of the people's court or the arbitration organization, the legally effective judgment of the people's court or the arbitration organization prevails'.[42] A people's court, in its turn, will afford protection against cybersquatting only to well-known trademarks.[43]

In view of the recent trend of governments striving to assert control over ccTLD[44] as well as IDN,[45] this lack of uniform rules for domain name dispute resolution is only liable to persist.

4 Conclusion

The issue of language used online is intimately connected to international trade. It is simply profitable for a country to have the

---

39 'Internationalized Domain Names – Intellectual Property Considerations', *WIPO Briefing Paper, Multilingual Domain Names: Joint ITU/WIPO Symposium, Geneva, December 6–7, 2001*, available at <http://www.itu.int/mlds/briefingpaper/wipo/wipofinal3.pdf>.

40 See <http://www.cnnic.net.cn/en/index/0Q/index.htm>.

41 See <http://www.cnnic.net.cn/html/Dir/2003/11/27/1518.htm>.

42 Art. 28, <http://www.cnnic.net.cn/html/Dir/2004/08/13/2442.htm>.

43 See 'The Interpretations of the Supreme People's Court on Some Issues Concerning Specific Application of Laws in the Trial of Civil Cases Related to Disputes of Domain Names on the Computer Internet', promulgated on July 17, 2001, discussed in supra footnote 38 at 19.

44 See, e.g., 'South African domain name tug-of-war', *BBC News*, 26 June 26 2002, <http://news.bbc.co.uk/1/hi/business/2067709.stm>; Julia Barton, 'Ukraine's Domain in Dot-Dispute', *Wired News*, 22 June 2001, at <http://www.wired.com/news/politics/0,1283,44012,00.html>.

45 See, e.g., Hong Xue, 'The Voice of China: A Story of Chinese-Character Domain Names', *Cardozo Journal of International Comparative Law*, vol. 12, no. 2 (2004), p. 559.

world speaking its language: cultural domination brings along foreign markets craving for goods and services associated with the country's language and lifestyle: movies, music, news channels, computer games based on comic strips, fast-food chains, broadcasting rights for sports events, etc. While some countries are trying to dominate the global cultural (and thus economic) scene, others get increasingly protective. Hence cultural and economic nationalism, sometimes bordering on chauvinism comes into play. The threat of Internet fragmentation[46] is just one manifestation thereof. The only viable option to overcome such division along cultural lines at this point seems to be the intensification of dialogue within the Internet's self-governance and standardization bodies that are already striving to find solutions to the problems brought about by the advent of IDN.[47] Their failure would go against the vision of the Internet's pioneers who saw it as a borderless media and an instrument of building a true multicultural Knowledge Society worldwide.

References

Bettinger, Torsten (ed.), *Domain Name Law and Practice: An International Handbook*, Oxford University Press, 2005.

Lindsay, David, *International Domain Name Law*, Hart, 2007.

46 See, e.g., Gren Manuel and Leslie Chang, 'Verisign's Plan for Domain Names Could Cut Internet World in Two', at <http://www.joinwow.org/newsletter/16/fa2/>.

47 See Molly Torsen, 'The Domination of the English Language in the Global Village: Efforts to Further Develop the Internet by Populating It with Non-Latin-Based Languages', *Richmond Journal of Law & Technology*, vol. 12, no. 2 (2005).

CHAPTER 3
e-ADMINISTRATION

CURRENT PROBLEMS OF THE DIGITAL IDENTITY MANAGEMENT IN BULGARIA

Svetlana Vardeva[1]

1 Introduction

Identity management (IdM) has known several interpretations in the ICT industry and is now associated as the management of users credentials and how they might log onto an online system. Thus usually the term identity management is associated with the problems related to the identification in the cyber space. However, this view is quite narrow. Therefore identity management may be considered as the management of information (as held in a directory) that represents real life identified items (users, devices, services, etc.).[2]

With regard to the digital identity management in Bulgaria understood as identity management in Internet, the issue is still undeveloped and only few governmental rules are existing in this respect. Actually still the most common means of cyberspace identification is the username-password system. The smart cards are scarcely used and the only legislative regulations with regard to identification in Internet are related to the electronic signature. This

---

1 Centre of the Law of Information and Communication Technologies (CLICT), 39 Shesti Septemvri Str., Sofia 1000, Bulgaria, <svetlana.vardeva@clict.net>.

2 <http://en.wikipedia.org/wiki/Identity_management#Electronic_Identity_Management_.28IdM.29>.

is the reason why in this article the term 'digital identity management' will be discussed from a broader point of view and subject to review herein will be the existing in Bulgaria electronic means of identification as a whole. The purpose of the article is to focus on both the legislative and practical problems that presently occur in Bulgaria in respect of electronically-based ways of identification.

2 Legal framework

Currently the status of the digital identity management in Bulgaria is at a quite low stage. A lot of attempts have been made lately in order to bring the Bulgarian legislation in line with the European Union requirements and the world tendencies. With regard to that in the last few years several completely new legislative acts were adopted and other already existing acts were amended.

However, the regulatory framework related to the digital identity management in Bulgaria is still quite scarce and is comprised of the following acts:

— The Bulgarian Identity Documents Act (*promulgated in State Gazette, issue 93 form 11 August 1998, in force as of 1 April 1999, last amendments in State Gazette issue 52 from 29 June 2007*);

— The BULSTAT Register Act (*promulgated in State Gazette, issue 39 from 10 May 2005, in force as of 11 August 2005, last amendments in State Gazette issue 42 from 9 May 2007*);

— The Electronic Document and Electronic Signatures Act (*promulgated in State Gazette, issue 34 from 6 April 2001, in force as from 6 October 2001, last amendments in State Gazette, issue 34 from 25 April 2006*). The act implements the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures;

— The Commercial Register Acts (*promulgated in State Gazette, issue 34 from 25 April 2006, still not in force*). The Act has the purpose to bring into compliance the Bulgarian legislation with the requirements of First Council Directive 68/151/EEC of 9

March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community;

— The Electronic Governance Act (*promulgated in State Gazette, issue 46 from 12 June 2007, will be in force as from 13.06.2008*).

Secondary legislation has been adopted on the basis of the pointed above acts, namely:

— Ordinance No. 7 from 29.06.2006 on the cooperation between the BULSTAT register and other registers and information systems and on data access (*promulgated in State Gazette, issue 56 from 11 July 2006*);

— Ordinance on the certification services providers activity, the order for its termination and the requirements on the provision of certification services (*promulgated in State Gazette, issue 15 from 8 February 2002*);

— Ordinance on the requirements towards the algorithms for qualified electronic signature (*promulgated in State Gazette, issue 15 from 8 February 2002*);

— Ordinance on the order for registration of the certification service providers (*promulgated in State Gazette, issue 15 from 8 February 2002*);

— Ordinance No. 1 from 14.02.2007 on maintaining, keeping and accessing to the Commercial register (*promulgated in State Gazette, issue 18 from 27 February 2007, last amendments in State Gazette, issue 20 from 6 March 2007, still not in force*);

— Ordinance on the order and means for accessing the Commercial register ex officio (*promulgated in State Gazette, issue 95 from 24 November 2006, still not in force*);

— *Others.*

With regard to the current legislation the main aspects of the digital identity management in Bulgaria, viewed as including all presently

existing electronically-based means of identification, can be summarized and will be reviewed herein as follows:

1. e-ID cards/passports;
2. e-Cards for legal entities and persons performing independent activities;
3. Electronic signatures;
4. Electronic commercial register.

3 e-ID cards/passports

Contrary to the situation in many other countries, in Bulgaria e-ID cards do not exist. Thus, the conception for the digital identity card that is developing in many countries in the European Union is still not common in Bulgaria and actually there is almost no governmental strategy concerning the issue in question.

The matter is regulated by the Bulgarian Identity Documents Act (BADA). Currently Bulgaria does not issue any electronic ID cards to natural persons. The identification of the natural persons is performed on the basis of the traditional ('paper') ID card or driving licenses. These documents are only machine-readable but for the moment no efforts for their transformation in electronic format are foreseen.

The only exceptions concerns passports. With amendments of BADA[3] the issuance of passports with electronic information carrier (which will most probably be in the form of a microchip) is provided and should start as from 31.10.2007 in order to bring in line the Bulgarian law with the requirements of the EU legislation.[4] Thus all the data written in the machine – readable part of the traditional and

3 *State Gazette*, issue 105 from 22 December 2006.

4 Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, <http://eurlex.europa.eu/LexUriServ/site/en/ oj/2004/l_385/l_38520041229en00010006.pdf>.

currently used passports shall be contained in electronic form in the new passports, which is as follows:

— Type of the document;
— Issuing authority;
— Name of the document owner;[5]
— Number of the document;
— Citizenship of the owner;
— Date of birth of the owner;
— Gender of owner;
— Date of expiry of the document's validity;
— Unified Citizen Number/Personal Number of Foreigner (unique identifiers);
— Controlling digits of the pointed above data.

Except for this traditional data the electronic carrier shall hold also a scanned photograph and the fingerprints of the relevant person.

The BADA provides that the certificates for travelling abroad of the refugees and asylum seekers, persons without citizenship and persons with humanitarian status will also contain the described data in electronic format.

As the procedure of issuance of electronic passports has not yet started, the eventual problems that may occur are not yet identified. It is expected that the implementation of the new type of passports will not be fast as the passport is not an obligatory type of identification document in Bulgaria and most probably only persons wishing to travel outside the EU will apply for a passport in the following years.

With regard to the formats of the electronic data, an act of the Government should be issued in order to state them explicitly and in details. This act should be in compliance with the Recommendations of the International Civil Aviation Organisation (ICAO).[6]

---

5 Generally most of the Bulgarian citizens have three names.

6 Document 9303, Machine Readable Travel Documents, Part 1 – Machine Readable Passports; <http://www.icao.int/icao/en/assembl/a35/wp/wp011_en.pdf>.

4 e-Cards for legal entities and persons performing independent activities

The BULSTAT Register Act (BRA) provides for the issuance of identification cards to legal entities, as well as to natural persons performing an independent activity (i.e. lawyers, traders, etc.). This register contains all legal entities whether they are performing commercial activities or not and natural persons performing an independent activity (lawyers, public notaries, interpreters, architects, engineers, insurance agents, courts experts, private receivers, consultants, auditors, etc.) fulfilling the following requirements:

— perform professional activity on their behalf;
— are not registered as natural persons performing commercial activity;
— are self-insuring persons within the meaning of the Social Security Code.[7]

A BULSTAT number is given to all registered entities and a traditional paper ID card is issued. The BRA however provides for the possibility for issuance of ID cards with an incorporated microprocessor chip. It should be noted that this is only a possibility given to the entities and no requirement exists which obliges the holders of the BULSTAT ID cards to issue these electronic cards. So far, the issuance of BULSTAT cards with microprocessor chip is not popular as no practical advantages of owning such kind of card exist.

5 Electronic signatures

The Electronic Document and Electronic Signatures Act (EDESA) regulates the first form of electronic identity management existing in Bulgaria – the electronic signature. As outlined hereinabove, the

7 Promulgated in *State Gazette*, issue 110 from 17 December 1999, in force as of 01.01.2000, last amendments in *State Gazette*, issue 41 from 22 May 2007.

EDESA was adopted to implement the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. However, the Bulgarian act contains certain deviations from the Directive related to the types of the existing electronic signatures (*please see item 5.1.1 below*). These deviations, legislative errors and wrong practices cause serious problems with regard to the electronic signatures as a digital identity management tool, as follows:

— Problems caused by legislative errors. They are related to wrong implementation of the Directive 1999/93/EC, as well as to lack of the necessary activity of the relevant Bulgarian institutions;
— Problems caused by wrong practices. They are related to wrong enforcement of the EDASA.

These two types of problems precisely will be subject to review herein below.

5.1 Problems caused by legislative errors

5.1.1 *Background information*

The EDESA[8] recognizes three types of electronic signatures:

— (basic) electronic signatures;
— qualified electronic signatures;
— universal electronic signatures.

(Basic) electronic signature is any information, related to the electronic statement in a way, coordinated between the author and the addressee that is sufficiently secured with regard to the needs of the civil and commercial relations, and that:

a) reveals the identity of the author;
b) reveals the consent of the author of the electronic statement;
c) protects the content of the electronic statement from future amendments.

8 Art. 13 of the EDESA.

Qualified electronic signature is a transformed electronic statement included, added or connected logically with the same electronic statement before the transformation.

Universal electronic signature (UES) is a qualified signature the certificate for which is issued by a certification service provider, registered in the registrar kept by the Bulgarian Communications Regulation Commission (CRC).

These definitions clearly state that the types of electronic signatures provided in the Directive 1999/93/EC and the ones provided in the EDESA are different. Thus[9] the meaning of basic electronic signature under the Bulgarian EDESA is similar to the meaning of advanced electronic signature under the Directive. The electronic signature as defined under the Directive 1999/93/EC shall be considered an electronic signature under the Bulgarian Law. Provided the electronic message is followed by a basic (general) electronic signature under the meaning of the Directive 1999/93/EC, under the Bulgarian Law it shall be considered as kind of authentication information, but the message shall not be considered signed at all. Further, the advanced electronic signature under the Directive 1999/93/EC is close to the Bulgarian qualified electronic signature, while the universal electronic signature under the EDESA is a type of qualified electronic signature which is supported by a qualified certificate issued by a *registered* certification service provider.

(Basic) electronic signatures and qualified electronic signatures are given in Bulgaria the same legal effect as handwritten signatures,[10] except in cases where the titular (owner) or the addressee of the electronic statement is the state or a municipal authority. In the latter case only the UES is recognized as an equivalent to a handwritten one.

---

9 <http://ec.europa.eu/idabc/servlets/Doc?id=29072>.

10 The Bulgarian legislation gives a very strong effect to handwritten signatures. Where the document is not signed with a handwritten signature, respectively with an electronic signature to which the law gives the same effect, the author of such document shall be deemed unknown.

5.1.2 *Problems regarding the possibility of non-Bulgarian entities (natural persons and legal entities) to receive e-Government services*

As discussed in item 5.1.1 above, according to the EDESA only the UES may be used before state or municipal institutions in Bulgaria in order to receive any e-Government service. Electronic signatures of foreign persons and entities issued not by Bulgarian providers as UES, are not recognised. He/she will have to acquire a UES within the meaning of the EDESA, i.e. an electronic signature, issued by a certification service provider registered with the Bulgarian CRC.[11]

5.1.3 *Problems regarding the possibility of receiving e-Government services by the Bulgarian judicial system authorities*

According to the EDESA[12] the acceptance and the issuance in the judicial system of documents signed with UES shall be regulated by a special legislation. Thus, for the time being, the provisions of the EDESA are not applicable to cases where the recipient or the author of the respective electronic document is a judicial authority. As no such legislation has been adopted currently only paper document may be submitted to these authorities.

5.2 Problems caused by wrong practices

5.2.1 *Background information*

All Bulgarian citizens have a unique identifier called Unified Citizen Number (UCN). It is a unique code, consisting of ten numbers which each Bulgarian citizen obtains as from his birth. A Bulgarian citizen may identify himself with the UCN before each institutions and persons in Bulgaria.

---

11 At present only four certification authorities are registered with the CRC. For more information: <http://www.crc.bg/>.

12 Art. 41, para. 2 of the EDESA.

Notwithstanding the fact that the UCN is the most common and reliable identifier, the EDESA does not require UCN to be included in the UES certificate. However, without a legal basis, most government applications currently use for identification the UCN. Certification service providers have commenced the wrong practice to include the UCN in the UES certificate.

5.2.2 *Problems regarding the untypical functions vested to the certification service providers*

As mentioned above most of the e-Government applications use the UCN for identification of their users. At providing information services the e-Government applications usually obtain the UCN and all the other necessary data from the certificate for the electronic signature of the relevant user. Thus an untypical function is imposed to the electronic signature certification service provider, namely to certify the identity of the signatories. It only must and is entitled to certify the connection between the author and the public key and has no other certification powers.

5.2.3 *Problems regarding the possibility of non-Bulgarian citizens to receive e-Government services*

The practice of the e-Government applications to use for identification of their users the UCN of the titular (owner) of the electronic signature reveals serious problems also in another aspect. It highly impedes the provision of e-Government services to foreign citizens, from other EU-member states included, as the UCN is a unique identifier only of the Bulgarian citizens. It practically results to a complete impossibility for foreign citizens to obtain Internet services from the Bulgarian institutions as they do not have a UCN.

Considering also the legislative obstacles before non-Bulgarian entities, examined in item 5.1.2 above, it may be concluded that the barriers for obtaining e-Government services by foreign citizens are really a lot and major steps must be taken for their elimination.

6 Commercial Register

6.1 Background information

At present all the legal entities, as well as the natural persons that perform commercial activity are registered with the Commercial Register of the District Court of the seat of the respective entity.[13] At registration with the court all the entities receive a company file number, comprised of a serial number combined with the respective year. Except for the BULSTAT number given at the BULSTAT registration (see part 3 above) this company file number is at the present moment also used as another type of traditional identifier. All the documents related to the status (past and current) of the entity are kept under the file numbers. Thus presently there are two parallel registers which use two different identifiers and all the entities specified above need to be registered in both of them, meaning they have to present one and the same information twice before different authorities (registers); they have to pay fees for each of the registrations, etc.

The commercial registers are still kept in 'paper' with no access by third parties. For that reason, the courts issue a paper called 'Certificate for good standing' on the basis of the registered data that is required in the relations with almost all state and municipal institutions.

6.2 The new Commercial Register

In order to bring the Bulgarian legislation in line with the requirement of the First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community, respectively to surmount the difficulties

13 Presently in the Commercial Registers kept with the District Courts are registered not only the commercial companies and the natural persons performing commercial activity but the non-profit organizations as well.

which the current identification system reveals, a completely new Commercial Register Act (CRA) was adopted on 24 March 2006.

6.2.1 *Basic principals under the CRA*

Under the CRA, commercial companies and natural persons performing commercial activity are registered in the new Commercial Register. The register has to be removed from the courts to be kept by a central administrative institution, namely the Registry Agency, and will be kept in electronic format.

In the future, a registration with the BULSTAT register will not be longer required. The commercial registration the data bases of the BULSTAT Register and of the current Commercial Registers will be consolidated in one unified electronic based register. The pointed entities shall receive a new unique identifier named Unified Identification Code (UIC). Once the new register starts working, the Registry Agency shall provide automatic access services to its data bases against a certain fee. The same services shall be provided free of charge to all state and municipal authorities, as well as to persons, performing public functions. Thus the current status and the relevant identifiers of the respective company shall be available electronically and be acquired by the authorities electronically.[14]

It should be however noted that non-profit organizations remain to be registered with the district courts, as well as with the BULSTAT register, respectively to receive two different identifiers. A BULSTAT registration shall be required also for the natural persons, performing an independent activity, as well as for partnerships, etc.

6.2.2 *Problems related to the new commercial register*

The major change from a paper to an electronic register has practically not yet started. Thus, still the old paper systems are used. According to the original text of the CRA the electronic register should have commenced working on 1 October 2006. As that was

14 Art. 23, para. 4 of the CRA.

not possible, its entry into force was suspended until 1 July 2007 and again until 1 January 2008.

The reasons for this delay are practical. The transformation is really enormous and a lot of resources (both human and technical) have to be involved in the process. However, such resources are not available. The political will for the implementation of the new regime is weak due to various reasons. Thus it is not certain that on 1 January 2008 Bulgaria will have an electronic commercial register. Until the availability the new register the present regime will be applicable, meaning the current problems will remain, i.e. various registrations; need to provide the same information to various authorities and institutions; payment of various fees for registrations, for obtaining 'paper' certificates for good standing, etc. These bureaucratic issues highly impede the activity of the entities by taking a great quantity of both human and financial resources.

7 Conclusion

The subjects discussed herein reveal the present situation in Bulgaria with regard to the state of electronically-based means of identification. Actually still the traditional ('paper') means of identification are preferred and broadly used. Though they are well developed during the years of practice and thus reliable, the new circumstances and technologies require the implementation and use of new (electronic) instruments. In this regard certain efforts has been made during the resent years but it still needs a lot to be done for the proper working of the new systems. There are no unified legislative rules in force regulating the development of the information systems of the state authorities and no coordination exists between them. Thus every administrative body applies its own particular rules for its e-Government services that are not in correspondence with the rules, practices and requirements of the other state bodies, including the rules with regard to identity management.

The difficult task to resolve at least some of the existing problems is assigned to the Electronic Governance Act which was adopted on 31 May 2007 and must enter into force as of 13 June 2008.

References

Dimitrov, George, 'Preliminary Study on Mutual Recognition of e-Signatures for e-Government applications, National Profile Bulgaria'. Please visit <http://ec.europa.eu/idabc/servlets/Doc?id =29072>.

Kalaidjiev, Angel, Borislav Belazelkov, Vesela Stancheva, George Dimitrov, Dimitar Markov and Maria Yordanova, *Electronic document and Electronic Signature. Legal Regime*, Sofia: Ciela Publishing, Center for Study of the Democracy, 2004.

PRINCIPLES OF IDENTITY MANAGEMENT UNDER THE NEW BULGARIAN e-GOVERNANCE ACT

Miroslav Ognyanov[1]

1 Introduction

e-Government in Bulgaria forms an element of the transition from industrial to information society. It is a process of change that helps expand the means of citizens and businesses to participate in a new, knowledge-based economy. In order to have the full potential of e-Government realized, it is necessary to reform information, the administration and the management of business processes. What is also needed is to change the mindset and line of action of public administration officials, as well as their work attitude and way of communication with citizens and businesses.

2 The history of e-Government in Bulgaria

2.1 Electronic Document and Electronic Signature Act

Several acts of different normative rank outline the legal framework of e-Government in Bulgaria.

---

1 LEX.BG JSCo., 132A G. S. Rakovski Str., fl.1, Sofia 1000, Bulgaria, <miroslav.ognyanov@lex.bg>.

In April 2001 the Electronic Document and Electronic Signature Act (EDESA) has been adopted. It lays down the usage of the electronic document, the electronic signature, and the conditions and order for provision of certification services.

The electronic document is defined by the EDESA as an electronic statement written down on a magnetic, optic or other carrier enabling reproduction. The electronic statement is expressed in a verbal statement presented in digital form. The written form shall be considered observed if an electronic document has been drawn up.

The electronic signature according to the EDESA is:

1. Any information related to the electronic statement in a way coordinated between the author and the addressee, secure enough with respect to the exchange, which:

   a) discloses the author's identity;
   b) discloses the author's consent with the electronic statement, and
   c) protects the contents of the electronic statement against subsequent changes;

2. The advanced electronic signature;

3. The universal electronic signature.

The electronic signature under items 1 and 2 has the validity of a handwritten signature unless the principal or addressee of the electronic statement is a state body or a body of the local self-government.

The universal electronic signature always has the validity of a handwritten signature notwithstanding the type of principal or addressee. The EDESA delegates to the Council of Ministers the right to determine which state bodies can use in their mutual relations some other type of electronic signature. To date such an act has not been passed.

To ensure fast and free document circulation, Art. 41, para. 1 of the EDESA assigns the Council of Ministers to determine its subordinate state authorities which should:

1. Be obliged not to refuse the receipt of electronic documents bearing a universal electronic signature;

2. Be obliged not to refuse the issuance of permits, licenses, approvals and other administrative acts in the form of electronic documents bearing a universal electronic signature.

Pursuant to Art. 41, para. 1 of the EDESA the Council of Ministers issued Ordinance No. 153 of 5th July 2004 for determining the bodies under Art. 41, para. 1 of the EDESA. All the Ministers, the National Statistical Institute and the National Social Security Institute are the addressees of this Ordinance.

The Ordinance applies only to the central administration and does not include local authorities and independent state authorities that are not subordinate to the Council of Ministers. Pursuant to Art. 41, para. 3 of the EDESA those authorities shall adopt Internal Rules for the acceptance and issuance of documents bearing a universal electronic signature. The above provision however has not been implemented in practice and the state bodies different from the central administration have not implemented rules for the acceptance and issuance of documents bearing a universal electronic signature.

Even though Art. 41, para. 2 of the EDESA provides for the adoption of an act regulating the usage of the electronic signature and the electronic document in the judiciary system, such an act does not exist yet. Thus the judiciary system is also excluded from the scope of application of the obligation under para. 1 of Art. 41.

The obligation of the central administrative authorities for acceptance and issuance of electronic documents has been in force since 01.01.2005. Thus the necessary preconditions for the initial use of the electronic document and the electronic signature in the relations with part of the administration have been created. In practice, the authorities having this obligation do not observe it properly. Part of the problem lies with the inadequate level of technical knowledge of the administrative personnel. However, the main reason for this non-performance is the poor condition of the technical equipment in the state administration.

2.2 e-Government Strategy

Even though the EDESA is a revolutionary act for the Bulgarian legislation, it is just the first step in the overall reform of the Bulgarian state administration, including district and municipal authorities. In 2002 the e-Government Strategy of the Republic of Bulgaria[2] was adopted with Resolution No. 866 of 28th December 2002 of the Council of Ministers, aiming to contribute to the implementation of information technologies in the state administration.

The main role of e-Government, stated in the Strategy, is to meet the general public's need for accessible high-quality public services. The e-Government development is also needed to increase transparency and minimize corruption practices in the state administration. Services should be provided in ways, at times and places convenient for citizens and businesses by an integrated and continuous electronic approach. Apart from the traditional communication channels, new types of communication platforms and devices are made available where the services shall be provided on a 'one-stop-shop' principle.[3] The Strategy envisages as customers of e-Government services citizens and businesses, as well as the public administration itself.

The implementation of contemporary information technologies in the government shall contribute to its modernization, upgrade its effectiveness and lead to cost reduction thus ensuring a possibility to meet the real needs of citizens and businesses at any time and any place, and expanding the technological possibilities for their participation in the governance. e-Government is meant to provide transparency in the public administration activities and opportunities for feedback as prerequisites for public control over the executive power.

---

2 English version available at <http://www.ccit.government.bg/common/documents/RetriveDocument.aspx?DocID=52&LanguageID=2> (visited 13 September 2007).

3 One Stop Shop Generic Model, adopted by a Council of Ministers Resolution no. 878 of 29 December 2002: <http://www.ccit.government.bg/common/documents/RetriveDocument.aspx?DocID=44&LanguageID=2> (visited 13 September 2007).

e-Government covers four major aspects of communication and services:

- Administration – Citizens: Modern Internet and Intranet web-based solutions coupled with conventional means for ensuring broad access, which shall lead to qualitative changes in the communication environment and service provision to citizens;
- Administration – Business: Modern solutions for optimization of processes and business relations between the public administration and various business entities;
- Administration – Administration: IT development at a national and interstate level with a view to ensuring effective interaction of various administrative structures;
- Internal Institutional Efficiency and Effectiveness: Organization and optimization of business processes, administration-personnel relations and communication processes within the administrative structures.

In each of these branches one of the main requirements to create an appropriate communication environment for the functioning of e-Government is to provide a reliable identification and information security system. The key points in this direction are:

- Data identification – establishment of proprietary data, responsibility for data authenticity and data exchange rules;
- Data security and protection – provision of maximum protection of the data processed and stored;
- Integrated approach – each project should conform to the overall idea of the Strategy and be part of an integrated system to ensure continuity and rule out duplication of projects;
- Single entry and multiple use of data – single entry of data by the authorized body and multiple use of such data in compliance with the legal regulations and access authorization.

2.3 Plan for the Implementation of the e-Government Strategy

In conformity with the e-Government Strategy, Plan for the Implementation of the e-Government Strategy in the period 2003–2005 was adopted with Resolution from 11th March 2004 of the Council of Ministers. The Plan execution and e-Government implementation are instruments for modernization of the public administration. The strategic targets of the Plan are:

- Provision of qualitative, economically effective and easily accessible administrative services to citizens and businesses electronically;
- Expansion of the technological possibilities of citizens and businesses to get involved in the state governance;
- Creation of an organizational, communication and information environment for effective and transparent functioning of the public administration in accordance with the principles, provisions and best practices of the European Union.

It is clear that these targets represent a logical development of the aims assigned by the Strategy. The Bulgarian government undertook to introduce by the end of 2005 20 indicative e-Government services for citizens and businesses (as defined by the European Commission) – 12 for citizens and 8 for businesses.

One of the main problems in implementing the Plan and the provision of the 20 indicative services is the lack of undertakings for specific financial arrangements. As a result, obvious from the below tables, the current implementation of the separate indicative services is at different levels of completion.[4]

---

4 Report on the e-Government in Bulgaria 2005: <http://www.ccit.government.bg/common/documents/RetriveDocument.aspx?DocID=356&LanguageID=1> (visited 13 September 2007).

Services for citizens

	Type of service	*Level of completion*
1	Income taxes: declarations, notifications	Fully completed
2	Services connected with seeking job opportunities at Labour Bureaus	Fully completed
3	Social insurance, unemployment benefits, children's allowance, medical expenses, scholarships	Fully completed
4	Personal documents: identity cards, passports, driving licenses	In process of development
5	Registration of motor vehicles	In process of development
6	Submission of documents for construction permits	In process of development
7	Petitions to the police (e.g. against theft, etc.)	Fully completed
8	Public libraries	In process of development
9	Certificates (of birth, marriage, etc.)	In process of development
10	Diplomas for secondary and university education	In process of development
11	Changes in address registration	Fully completed
12	Healthcare services	In process of development

Services for businesses

	Type of service	*Level of completion*
1	Social insurance for employees	Fully completed
2	Corporate taxes: declarations, notifications	Fully completed
3	VAT: declarations, notifications	Fully completed
4	Customs declarations	Fully completed
5	Incorporation of companies	In process of development
6	Sending data to the National Statistical Institute	In process of development
7	Permits related to environmental regulations	In process of development
8	Public procurement	In process of development

3 The Electronic Governance Act

The next step in the process of accomplishing the transition from the traditional administrative model to integrated electronic administrative services for citizens and businesses is the adoption of the Electronic Governance Act (EGA). The act was promulgated in State Gazette, issue 46 from 12.06.2007, but its entry into force is delayed until 13.06.2008. It formulates the main principles of electronically-based administrative procedures.

The EGA lays down the activity of the administrative bodies as regards electronic documents, provision of electronic administrative services and exchange of electronic documents among the administrative bodies.

It is important to note that the EGA regulates not only the work of state authorities but also applies to the activities of persons charged with public functions and organizations providing public services. The definitions of these persons and organizations are provided in paragraph 1, items 11 and 14 of the Additional Provisions of the EGA. *Persons charged with public functions* are public notaries, private receivers, state and municipal educational establishments, state and municipal healthcare establishments and other persons and organizations through which the state performs its functions as specified by law.

Organizations providing public services do not need to be incorporated in a specific form stipulated by law. These can involve any kind of legal entities that provide educational, healthcare services, water, energy and gas supply, telecommunication, post and other similar services, in the course of provision of which administrative services might be rendered.

The EGA is inapplicable when the legislation stipulates a specific form or procedure for the execution of certain actions. For instance, according to the Bulgarian Contracts and Obligations Act, the purchase contract for a real estate shall be concluded in the form of a notary deed. Although the public notary is a person charged with public function and the EGA is normally applicable to its services, the specific procedure of signing the notary deed in person before the notary excludes the application of electronic services in this case.

The EGA does not cancel the rules for work with paper documents. Citizens and businesses can always choose between modern administrative attendance by means of electronic services and the traditional usage of paper documents.

4 Main principles of the EGA

Some of the principles established in the e-Government Strategy are legislatively developed by the EGA. The EGA formulates the following main principles:

4.1 Obligatory receipt and issuance of electronic documents and obligatory provision of electronic administrative services (Art. 10 of the EGA)

The essence of this principle is the general prohibition for providers of electronic administrative services (the meaning of the term is described below) to refuse the acceptance of electronic documents, issued and signed in conformity with the requirements of the EDESA and the EGA, as well as to refuse the issuance of electronic documents and provision of electronic administrative services.

On analyzing this principle the definitions relevant to its contents need to be clarified. *Administrative services* comprise the following actions:

a) issuance of individual administrative acts certifying facts of legal importance;
b) issuance of individual administrative acts which verify or deny the existence of rights or obligations;
c) accomplishment of other administrative actions in which natural persons or legal entities are rightfully interested;
d) consultations on an administrative legal regime, provided under a legislative act or concerning the issuance of an administrative act or the provision of some other administrative service, which represent a rightful interest for a natural person or a legal entity;
e) expert reports representing a rightful interest for a natural person or a legal entity when a legislative act stipulates their preparation as an obligation of a state authority administration or an authorized organization.

According to Art. 8, para. 1 of the EGA, *electronic administrative services (EAS)* are administrative services provided to citizens and organizations by the administrative bodies, services provided by persons charged with public functions and public services which can be requested and/or provided distantly, by electronic means.

Electronic services are provided by the so-called *providers of electronic administrative services (PEAS),* which can be:

— Administrative bodies;
— Persons charged with public functions;
— Organizations providing public services.

The providers supply electronic services within their competence to citizens and organizations – recipients of electronic administrative services.

The PEAS must provide all the services within their competence electronically as well, unless a special form for conducting certain actions or the issuance of relevant acts is stipulated by law.

When the special form has legal relevance, but part of the service may be requested or provided electronically, the PEAS shall provide such opportunity.

By obliging the PEAS to act under the conditions of limited competence as regards the choice of preferred means for administrative attendance, this principle provides for the use of modern information technologies in the administrative procedures. Thus, the costs, the time consumed and the complexity of the procedures for provision of services are essentially reduced. The lack of discretionary power of the administrative bodies to choose whether they shall provide services within their competence electronically or not, places recipients in an equal position, thus being an expression of the unified administrative approach to citizens and businesses.

4.2 Single collection and creation of data (Art. 2 of the EGA)

This principle means that the PEAS cannot require of citizens and organizations to produce or prove data which have already been collected or created. They shall collect such data *ex officio* from the primary data administrator. Art. 2, para. 2 of the EGA explains the notion of *primary data administrator (PDA)* – an administrative body, which under the law collects or creates, for the first time, data about natural persons or organizations, and processes or deletes such data.

Regardless of the factual difficulties connected with the implementation of this principle, it is a significant decision for the actual state of the Bulgarian administration. It directs administrative processes in favour of citizens and businesses, saves time and reduces the negative emotions in communicating with the administration.

4.3 *Ex officio* submission (Art. 3 of the EGA)

Administrative bodies shall request the necessary data from the PDA. The latter shall submit *ex officio* the requested data to all administrative bodies, persons charged with public functions and organizations providing public services, which, on a legal basis, process these data and have expressed the will to obtain such.

This principle is related to the establishment of integrated administrative attendance, i.e. administrative attendance using integrated information within the framework of one administration, as well as between an individual administration and/or a legal entity providing public services by means of an information register.

The *ex officio* submission is part of the organizational principle for 'one-stop-shop' attendance. The two main means for fulfillment of this principle are:

— one place for access to one administrative structure;

— one place for access to several 'horizontal' administrations.

4.4 Automated data transmission (Art. 4, para. 1 of the EGA)

The notification and request for data transmission in providing electronic administrative services shall be carried out automatically by electronic means as an internal electronic administrative service. Section 1, item 4 of the EGA gives the definition for *internal electronic administrative service* – administrative service which an administrative body provides to another such body to complement the latter's competence. According to Art. 39, para. 1 of the EGA it is necessary that these services be requested and/or provided distantly, by electronic means. They can be provided by administrative bodies as

well as by persons charged with public functions and organizations providing public services.

Each institution adopts its internal rules for work with electronic documents which shall be applied upon provision of internal electronic services.

The implementation of the principle shall be ensured by a National Asynchronous Transfer Mode Network which is in process of development. An integrated optical communication network linking ministries and other state agencies in Sofia is already in operation. The extension of this network to the regional centers of Bulgaria is currently under way.

4.5 Obligation to specify a Unique Identifier (Art. 5 of the EGA)

Only citizens, respectively organizations that have indicated their unique identifiers shall be able to take advantage of electronic administrative services. All providers of such services undertake to provide a possibility for citizens and organizations to specify a unique identifier upon applying for the respective electronic administrative service. This obligation of citizens and organizations using administrative services by electronic means is of great significance since it guarantees the secure circulation of documents as regards authorship and protects from abuses.

Four types of *unique identifiers* are specified in para. 1, item 22 of Additional Provisions of the EGA:

— Personal Identification Number of Bulgarian citizens and foreign natural persons residing permanently on the territory of the Republic of Bulgaria. As from his/her birth each Bulgarian citizen has his/her administrative identifier called Personal Identification Number, given by the civil status official in the respective municipality for the purposes of civil registration. According to the Citizen Registration Act all Bulgarian citizens and the most important facts related to natural persons – birth, marriage and death – shall be registered into

the Civil Status Registers. Containing the data already specified, civil registration helps for the individualization of every natural person as a holder of subjective rights.

— Personal number of a foreigner – for foreign natural persons who have been granted long-term stay;

— Uniform identification code of companies and subsidiaries of foreign companies. As of 01.01.2008 a new Commercial Register Act shall become effective. Under this act the legal entities which are commercial companies shall have a unique identification code and this should be their only identifier.

— The BULSTAT code – for persons subject to entry in the BULSTAT Register. The BULSTAT Register represents a state register containing detailed data about legal entities and natural persons of specific capacity enumerated in the BULSTAT Register Act. When the new Commercial Register Act takes effect, all the legal entities which are commercial companies shall have a unique identification code based on the former BULSTAT code. As of 01.01.2008 only legal entities or subsidiaries of such entities which are not commercial companies and natural persons of specific capacity shall have a BULSTAT code.

5 Identity Management

In deciding to use electronic administrative services, citizens and businesses make electronic statements addressed to the administrative bodies, which should be issued and signed in compliance with the EDESA provisions. Pursuant to Art. 22, para. 2 of the EGA the integrity and authorship of statements lodged electronically as regards electronic administrative services shall be ascertained by an electronic signature.

In electronic communication issues related to ascertaining and guaranteeing the statements authorship and integrity turn out to be fundamental.

The electronic signature represents an asymmetric cryptographic system involving the use of two keys – a private and a public key. The private key is algorithmically bound with the public key. Using the first key the statement is encoded and the function of the public key is to make the message readable. By the use of the public key it can be ascertained whether the transformation of the initial electronic statement is done by using its respective private key and also whether the statement has been changed after the transformation.

With respect to the use of electronic administrative services, Art. 23 of the EGA requires that the electronic signature certificates issued specify the exact full name of the author's electronic signature, and in cases when the certificate contains data about a principal – the full name of the latter as well. An author and a principal of the electronic statement are terms used in EDESA – as per Art. 4 of the EDESA an author of an electronic statement is a natural person who is specified in the statement as its performer. A principal of an electronic statement is the person on whose behalf the electronic statement has been made.

When the electronic signature certificate indicates that the applicant, 'author', is acting on behalf of another person, 'principal', the grounds of empowerment shall be indicated in the certificate. If the empowerment ensues from other authorized persons, the certificate must contain data about these persons too.

It is possible to use a certificate not containing any data about the grounds of authorization despite the fact that the author and the principal of the statement are different persons. In this case the applicant must indicate in the electronic statement that he/she acts on behalf of the administrative service recipient. When the representative power is not stemming from the law, its scope shall be established by the text of the electronic statement. To guarantee the interests of the service principal and the public, the ECA provides that the applicant shall bear criminal liability under the Penal Code for declaration of untrue circumstances. Providers of electronic administrative services have in turn the obligation to ensure the opportunity for authors to specify in the electronic statements the capacity in which they are acting.

The identity check of the applicants for electronic administrative services is possible through the use of the electronic signature certificates. The electronic signature certificate represents formatted data which connects a particular subscriber (natural person or legal entity) with his/her public key. The electronic signature certificate ensures:

- Authenticity – identification of the parties in contact;
- Integrity – the document is not changed on its way through the Internet;
- Privacy – confidential information can be sent and accessed only by the interacting parties;
- Unavoidability – the correspondents are authors and cannot deny the statements made;
- Time-saving – the time spent for the activity is reduced, resulting into lower costs.

To date the Communications Regulation Commission has registered four providers of certifying services for the universal electronic signature in Bulgaria on the grounds of Art. 34, para. 1, item 1 of the EDESA.[5] As mentioned above, only universal electronic signatures are accepted as equivalent of handwritten signatures in communication with public authorities under applicable Bulgarian legislation and respectively only certificates to such universal electronic certificates could be used for the purposes of identity check of recipients of electronic administrative services.

Pursuant to Art. 28, para. 1 of the EGA, when a request is lodged electronically, the PEAS shall verify the applicant's identity. During the check the applicant's name specified in the request is compared with the author's name contained in the electronic signature certificate. If the applicant is a natural person the provider also makes a check in the respective administration responsible for the personal registration of natural persons whether the natural person's name contained in the

5 Register available at <http://www.crc.bg/v1/files/bg/964.htm> (visited 13 September 2007).

electronic signature certificate corresponds to the unique identifier that the applicant has specified in accordance with Art. 5 of the EGA.

Identity verification of legal persons shall be carried out through checks in the respective registers of legal persons. Currently the commercial registers of merchants are kept on paper by the regional courts. However, the new Commercial Register Act provides that as of 01.01.2008 the centralized commercial register shall be kept by an administrative body – the Registry Agency – and will exist only in an electronic form, which would make possible automated electronic checks by administrative bodies for the purposes of provision of electronic administrative services.

The identity check principle in provision of e-Government services is not absolute and has certain limits established by the EGA. The exception provided by the law refers to those cases, when administrative service can be carried out without identity verification of the applicant. In such cases no identity check is needed.

When the identity check is required by law but the applicant cannot identify himself/herself, has not specified his/her unique identifier or has not used a universal electronic signature in compliance with the EDESA rules, a message shall be sent to him/her stating that the receipt of his/her application is not confirmed and the reasons thereof.

The importance of the identity check through the use of unique identifier is related to its central place in the system of new principles of provision of administrative services. In the times of provision 'paper' administrative services the applicant was obliged to provide evidence to the provider of the service for every single fact of legal value – i.e. he had to present together with his applications various certificates and acts issued by other administrative bodies. With the introduction by the EGA of the principles of single collection and creation of data and *ex officio* submission (sections 4.2 and 4.3 above) the burden of collection of all the relevant information is shifted from the citizen/the service recipient to the administrative body/the service provider. The principle of automated data transmission (section 4.4 above) assists the smooth and fast provision of the administrative service.

The ultimate purpose of the new system of electronic administrative service provision is to save time and costs to the citizens and organizations and to reduce the negative emotions in their contact with administration. Here comes the central question of applicant's identity management. Having verified the applicant's identity through his unique identifier, the state authority is able to assist him in exercising his rights and can obtain directly from the primary data administrator all the information needed for provision of the requested electronic administrative service.

To avoid any risk for misuse of the principles of single data collection and automated data transmission, the EGA creates several safeguards of the system, ensuring that the privacy of the citizens will be protected. One of those safeguards is the rule that internal administrative services are provided only in case of request by the authority, never automatically, and only to bodies that are empowered by the law to process the data exchanged (Art. 3 of the EGA). The EGA does not derogate the rules of the Personal Data Protection Act (PDPA) which are fully applicable in the provision of electronic administrative services and internal electronic administrative services. The providers of electronic administrative services and primary data administrators have all the obligations of data controllers as provided in the PDPA and the law guarantees the protection of natural persons' rights in processing their personal data.

Another safeguard stipulated in the EGA to protect the personal data and privacy of citizens are the provisions determining the security of the provision of administrative services. Section III from Chapter Four of the EGA ('Information Security') contains the rules that ensure the security of the information systems used in the process of providing electronic administrative services. The Chairman of the State Agency for Information Technologies and Communications is empowered to certify the information systems used by the state authorities. Under Art. 43 of the EGA the Council of Ministers shall issue an Ordinance for the condition and standards of information security in EAS provision, which will further develop the concept for information security outlined in the law.

6 Future Steps

The adoption of the EGA, even though preceded by some preliminary steps, is just the beginning of the real reform in the state governance in Bulgaria and the introduction of the new principles of electronic administrative service provision and identity management. There are more than a dozen of acts of secondary legislation under the EGA that shall be adopted until 12.12.2007 (i.e. within six months of publication of the law). Until the same deadline the Chairman of the State Agency for Information Technologies and Communications shall audit the information systems of all administrations and make recommendations on the basis of the audit. As a result, the administrative bodies shall bring their information systems into compliance with the Chairman's recommendations and the EGA standards not later than the EGA's coming into force on 13.06.2008.

Only the timely adoption of the acts of secondary legislation and the effective actions of the administrative bodies for reorganization of their information systems could lead to the effective implementation of the new rules and principles of the EGA. For the successful completion of the process large scale work should be undertaken in very tight deadlines, aiming to compensate the delay of the administrative reform in the country. The time until the entry into force of the new legal framework also gives a chance to make the necessary amendments and supplementations to the provisions of the law, thus correcting possible mistakes and omissions found in the process of preparation for its implementation. Upon successful completion of all this preparatory work the entry of the EGA in force in June 2008 will mark the start of the revolutionary modernization of the work of the administration, taking it from the paper world into the digital era of paperless environment and fast, effective and client oriented administrative services.

References

Димитров, Г., 'С Лице към хората: Закон за електронното управление (проект)', <http://www.mdaar.government.bg/docs/E-governance%20Act-FINALL.ppt#339,1>, С лице към хората.

Калайджиев, А., Белазелков, Б., Станчева, В., Димитров, Г., Марков, Д., Йорданова, М., *Електронният документ и електронният подпис* (Сиела Софт енд Пъблишинг: София 2004).

CHAPTER 4
e-JUSTICE

AROUND A RIGHT ROAD: THE PROGRESSIVE SPANISH IMPLEMENTATION OF NEW TECHNOLOGIES IN THE ADMINISTRATION OF JUSTICE

Nicolás Cabezudo Rodríguez[1]

1 Matter of fact

First of all, I must emphasized that the generalization of technological mechanisms in the Spanish Administration of Justice, later that in the private sector, is already a reality. As it is logical, the usefulness verified by the new technical advances has been the main factor of the impulse that this issue has received in the last years.

The true thing is that the position of the Administration of Justice has evolved from the scepticism to a passion, sometimes immoderate, as regards the use of the technological advances to satisfy its own needs. We refer to the infrastructural facet, relative to the endowment and development of the material resources directed to the administrative management of the procedures. We must clarify it because it still subsists some rejection relative to the functional aspects of that phenomenon, for instance when the courts have to allow that technologies like evidence.[2]

---

1 Universidad de Valladolid.

2 See our opinion in Cabezudo Rodríguez (2004: 1).

That process is clear when we speak about informatics resources and communication technologies, where we are living a real revolution.[3] But I'm not going to dedicate this presentation to those mechanisms but to the use of other new technological tools into the administration of Justice prompted by the last legal reforms in Spain. In fact, we will speak about the video documentation in the civil procedures (article 147 Spanish Civil Procedure Act – LEC –); the use of electronic bracelet in enforcement of criminal judgements (articles 33.4 y 37 Spanish Criminal Code – CP – y RD 515/2005, May the 6th, and 86.4 Spanish Penitentiary Statute, RD 190/1996), and others technological devices, as the 'computerized judicial memo' (article 796.1.3ª, 4ª y 5ª Spanish Criminal Procedure Act – LECrim. –) or the videoconference (articles 229 y 230 LOPJ y 306, 325 y 731 bis LECrim.). Nowadays, all of those technical facilities are available and widely used in Spanish Administration of Justice.

The aim of this presentation is analyze briefly each of those instruments.

2 Video documentation in the civil procedures

Until Spanish Civil Procedure Act of 2000 the clerk of the court had to elaborate by hand, physically, the records of trial. From then recording in video of the public hearing, certified by the clerk, replaces written records (article 147 LEC).[4]

---

3 I am talking about informatics' systems like MINERVA (management) or LEXNET (communications), and other, which goal is to achieve the so called 'principle of electronic continuity', that it will make feasible the electronic submission of writings and documents to the courts, who will give similar treatment to them. See Cabezudo Rodríguez (2006: 615).

4 Literally: 'Artículo 147. Documentación de las actuaciones mediante sistemas de grabación y reproducción de la imagen y el sonido. Las actuaciones orales en vistas y comparecencias se registrarán en soporte apto para la grabación y reproducción del sonido y de la imagen.

La grabación se efectuará bajo la fe del Secretario Judicial, a quien corresponderá la custodia de las cintas, discos o dispositivos en los que la grabación se hubiere efectuado.

Las partes podrán pedir, a su costa, copia de las grabaciones originales'.

Technically, it has been chosen by a system of double camera, one located in the head of the courtroom and another one in the opposed place of the room, in addition to that is being come to the gradual substitution of the initial video recording by DVD, which assist its file and conservation, previously to its digitalization.

Although it is not exactly the same to be present at the proceedings that to contemplate them in a screen, the advantages of that rule are clears, mainly because video record of trial, especially in relation to proof, it is always more reliable than a written transcription of which there has happened. It assist the analysis of the evidence by the court of first instance and its later control on appeal, prolonging the immediacy, above all in systems of limited appeal as it's the Spanish legal procedure, where the trial is not celebrated in again before the court of second instance. Even, this innovating system of documentation will allow the extension of the publicity of proceedings away from the own hearing, even for no parties in litigation, so the community in general.[5]

The recognition of the video record as official document is still a question unsolved. At the present time, only the written transcript will have that legal nature, being able to give the paradoxical situation of which if they were appraised contradictions between the transcribed material and the original one prevail the written version.

In any case, the implementation of that mechanism to other jurisdictions, mainly criminal and labour jurisdictions, is revealed highly suitable. The last enacted reforms of the criminal procedure make obvious that this argument is, at least partly, shared by the Lawmaker, especially, the disposition relative to preventive video recording of witnesses and victims depositions if for whatever reason it is anticipated that it will not be feasible to examine any evidence in

5 About those advantages see Gómez Martínez [2007].

the trial or will be cause of adjournment of a sitting[6] (articles 777.2[7] y 797.2[8] LECrim.).

3 Electronic Mechanisms for Inmates Monitoring (Electronic Bracelet)

Although it was not implemented until 2000 for technical reasons, the use of devices of electronic surveillance for the control of inmates was anticipated already in the Spanish Penitentiary Statute of 1996 (RD 190/1996, February the ninth, article 86.4).[9]

The rule at issue covers inmates who are at the end of their institutional sentence, classified in third degree of treatment and open-plan of imprisonment, and when the convict is developing a job outside of prison.[10] Basically, it is a '*Back-Door System*',[11] which main goal is to advance the conditional release to the inmates. It implies

---

6 Literally: 'fuere de temer razonablemente que una prueba no podrá practicarse en el juicio oral, o pudiera motivar su suspensión'.

7 The article 777 literally said: '[…] 2. Cuando, por razón del lugar de residencia de un testigo o víctima, o por otro motivo, fuere de temer razonablemente que una prueba no podrá practicarse en el juicio oral, o pudiera motivar su suspensión, el Juez de Instrucción practicará inmediatamente la misma, asegurando en todo caso la posibilidad de contradicción de las partes.

Dicha diligencia deberá documentarse en soporte apto para la grabación y reproducción del sonido y de la imagen o por medio de acta autorizada por el Secretario judicial, con expresión de los intervinientes.

A efectos de su valoración como prueba en sentencia, la parte a quien interese deberá instar en el juicio oral la reproducción de la grabación o la lectura literal de la diligencia, en los términos del artículo 730'.

8 The article 797.2 is similar than the article 777.2, although in this case is applied to a kind of judicial enquiry so called 'urgent proceedings'.

9 The 'Instrucción de la Dirección General de Instituciones Penitenciarias 13/2001', of December the 10th, regulates the material aspects for its implementation.

10 About those requirements see chapter III, title III of Penitentiary Statute.

11 Different than 'Front-Door System' used in probation. Although tests with other aims had been made previously, like those of Ralf Schwitzgebel in 1964 for the control of mental patients, the origin of these systems for the supervision of inmates, commonly known as 'electronic jail o prison' is located in the United States of North America in the beginning of the 80s.

that if the inmate accepts to carry a monitoring device, as it is the electronic bracelet, he will be exempted to spend the night in prison, being only required to return to complete his program of individualized treatment. The administrative decision is taken by a Technical Committee in prison and it can be review by the courts.

Between the different useful technologies, in Spain, it has been preferred a 'continuous signalling system',[12] which allows the free movement of the individual inside a certain area electronically controlled, in this case his own residence.

As much the penitentiary system as a whole as the inmates obtain significant benefits of this technological mechanism. In this sense, that situation of release will most probably help the rehabilitation of the offenders because make possible its family and social relations or the access to the labour market, without overlooking that it implied a decrease of the financial cost of incarceration, in addition being known the problem of prison overpopulation. A careful selection of the candidates will be a transcendental factor in the success of this alternative method of criminal enforcement.[13]

However, it should also be pointed out that electronic monitors alone are insufficient to enforce adequately a home confinement program. There also needs to be personal involvement with the offender on the part of a supervising officer to assure that the offenders satisfy its duties, like working or not keep in illegal behaviour.[14]

Anyway, that electronic device of control is a system of unlimited possibilities in other areas, like to guarantee the satisfaction of certain penalties, intermediate sanctions such as for instance the permanent

---

12 Usually it is distinguished between passive systems, such as the 'programmed contact system' based in aleatory telephone calls; 'global positioning system' based in GPS technology, and the active system aforementioned. See Gudín Rodríguez-Magariños (2005); Iglesias Río and Pérez Parente (2005: 412–15). Poza Cisneros (2002: 59) make a very important comparative study of common law and civil law systems.

13 See 'Instrucción 13/2001', pp. 3–4.

14 Klein-Saffran [2007].

location penalty (articles 33[15] and specially 35[16] of the CP), or in order to assure provisional measures, such as 'remove' or 'estrangement' measure (article 544 *bis* of LECrim.).[17] The use of technologies based on GPS, 'global positioning system', will increase its advantages and their implementation in these matters.

4 Computerized judicial MEMO

The 'computerized judicial memo' is a device by means of that the police officers know the trial calendar of each night court, allowing them to manage it.

The starting point was the 2002 Reform Act of the Criminal Procedure that supposed an extension of the Police powers, mainly inside a summary procedure so called 'Fast Trial',[18] where those enforcement officers assume, in addition to other duties, the subpoena before the night courts of defendants and victims, as well as of the witnesses and experts (article 796.1.3ª, 4ª y 5ª LECrim.).

In order to fulfil that task satisfactorily, direct communications between the referred Police and the Courts were necessary, at least so that officers knew the predicted setting dates for trial. That

---

15 Where are enumerated the different kinds of criminal penalties.

16 Literally: 'Son penas privativas de libertad la prisión, la localización permanente y la responsabilidad personal subsidiaria por impago de multa'.

17 Literally: 'En los casos en los que se investigue un delito de los mencionados en el artículo 57 del Código Penal, el Juez o Tribunal podrá, de forma motivada y cuando resulte estrictamente necesario al fin de protección de la víctima, imponer cautelarmente al inculpado la prohibición de residir en un determinado lugar, barrio, municipio, provincia u otra entidad local, o Comunidad Autónoma.

En las mismas condiciones podrá imponerle cautelarmente la prohibición de acudir a determinados lugares, barrios, municipios, provincias u otras entidades locales o Comunidades Autónomas o de aproximarse o comunicarse, con la graduación que sea precisa, a determinadas personas […]'.

18 That procedure, in compliance with the provisions of article 795 LECrim., covers fragrant and easy investigations cases in less serious offences (less than 5 years of imprisonment) such as certain crimes against persons (physical and psychological injuries), property (as larcenies, cars theft…), road traffic offences, and others.

'judicial memo' will provide that information to them and it will allow them to fix the day, the hour and court before which all they – defendants, victims, witnesses and experts – will have to appear, giving them, in the same act, an official writ.

Nowadays, the past problems relative to the coordination between the different police bodies are solved,[19] although others caused by the creation of new special courts, so called Courts of gender violence (violence against women), subsist because of its jurisdiction affects on the affair distribution to the night courts, making that kind of the police task more complex and increasing the possibilities of mispresentation, particularly because the officers must do a pre-selection of the charges, classifying the case *prima facie* and presenting it before the competent court. There can be no doubt that it will be necessary to develop specific programs to train police officers to take this legal decision, which, it is clear, is one of the more determinant factors of the reform success.

5 Videoconference

Although from 1994 Reform (LO 16/1994) of the Spanish Judicial Power Act (LOPJ) the use of videoconference as alternative method to appear physically before the court had cause of action (article 230),[20] it is with the 2003 Reform Act of Criminal Procedure (LO

19 A practical problem was that certain Police Bodies (Cuerpo Nacional de Policía and Guardia Civil) hold that judicial memo while other didn't it (Local and Regional Police), so the last one had to use the traditional written system. What required the elaboration of 'guidelines' by the Technical Committee of the National Commission of Coordination of the Judicial Police so called: *Criterios para la práctica de diligencias por la Policía Judicial en aplicación de la Ley 38/2002, de 24 de octubre, de reforma parcial de la Ley de Enjuiciamiento Criminal, sobre el procedimiento para el enjuiciamiento rápido e inmediato de determinados delitos y faltas, y de modificación del procedimiento abreviado.* About that document and the coordination problems see Pedraz Penalva (2003: 50–1).

20 Literally: '1. Los Juzgados y Tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establece la Ley Orgánica 5/1992, de 29 de octubre, y demás leyes que resulten de aplicación.

13/2003), when it arises a specific regulation related to criminal jurisdiction that extends and makes explicit the previous general rule.[21] In addition, videoconference is one of the specific form of mutual assistance foresee in the EU Convention on Mutual Assistance in Criminal Matters, 29 of May of 2000 (article 10).[22]

---

2. Los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

3. Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la Ley.

4. Las personas que demanden la tutela judicial de sus derechos e intereses podrán relacionarse con la Administración de Justicia a través de los medios técnicos a que se refiere el apartado primero cuando sean compatibles con los que dispongan los Juzgados y Tribunales y se respeten las garantías y requisitos previstos en el procedimiento que se trate.

5. Reglamentariamente se determinarán por el Consejo General del Poder Judicial los requisitos y demás condiciones que afecten al establecimiento y gestión de los ficheros automatizados que se encuentren bajo la responsabilidad de los órganos judiciales de forma que se asegure el cumplimiento de las garantías y derechos establecidos en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los Datos de Carácter Personal'.

21 About the Spanish National Plan see Giménez Ontañón (2003).

22 The article 10 regulates in detail that form of assistance.

'Hearing by videoconference:

1. If a person is in one Member State's territory and has to be heard as a witness or expert by the judicial authorities of another Member State, the latter may, where it is not desirable or possible for the person to be heard to appear in its territory in person, request that the hearing take place by videoconference, as provided for in paragraphs 2 to 8.

2. The requested Member State shall agree to the hearing by videoconference provided that the use of the videoconference is not contrary to fundamental principles of its law and on condition that it has the technical means to carry out the hearing. If the requested Member State has no access to the technical means for videoconferencing, such means may be made available to it by the requesting Member State by mutual agreement.

3. Requests for a hearing by videoconference shall contain, in addition to the information referred to in Article 14 of the European Mutual Assistance Convention and Article 37 of the Benelux Treaty, the reason why it is not desirable or possible for the witness or expert to attend in person, the name of the judicial authority and of the persons who will be conducting the hearing.

4. The judicial authority of the requested Member State shall summon the person concerned to appear in accordance with the forms laid down by its law.

Reform Act, as general criterion, introduces a new section in article 229 of the Spanish Judicial Power Act, empowering the Courts the

---

5. With reference to hearing by videoconference, the following rules shall apply:

(a) a judicial authority of the requested Member State shall be present during the hearing, where necessary assisted by an interpreter, and shall also be responsible for ensuring both the identification of the person to be heard and respect for the fundamental principles of the law of the requested Member State. If the judicial authority of the requested Member State is of the view that during the hearing the fundamental principles of the law of the requested Member State are being infringed, it shall immediately take the necessary measures to ensure that the hearing continues in accordance with the said principles;

(b) measures for the protection of the person to be heard shall be agreed, where necessary, between the competent authorities of the requesting and the requested Member States;

(c) the hearing shall be conducted directly by, or under the direction of, the judicial authority of the requesting Member State in accordance with its own laws;

(d) at the request of the requesting Member State or the person to be heard the requested Member State shall ensure that the person to be heard is assisted by an interpreter, if necessary;

(e) the person to be heard may claim the right not to testify which would accrue to him or her under the law of either the requested or the requesting Member State.

6. Without prejudice to any measures agreed for the protection of the persons, the judicial authority of the requested Member State shall on the conclusion of the hearing draw up minutes indicating the date and place of the hearing, the identity of the person heard, the identities and functions of all other persons in the requested Member State participating in the hearing, any oaths taken and the technical conditions under which the hearing took place. The document shall be forwarded by the competent authority of the requested Member State to the competent authority of the requesting Member State.

7. The cost of establishing the video link, costs related to the servicing of the video link in the requested Member State, the remuneration of interpreters provided by it and allowances to witnesses and experts and their travelling expenses in the requested Member State shall be refunded by the requesting Member State to the requested Member State, unless the latter waives the refunding of all or some of these expenses.

8. Each Member State shall take the necessary measures to ensure that, where witnesses or experts are being heard within its territory in accordance with this Article and refuse to testify when under an obligation to testify or do not testify according to the truth, its national law applies in the same way as if the hearing took place in a national procedure.

9. Member States may at their discretion also apply the provisions of this Article, where appropriate and with the agreement of their competent judicial authorities, to hearings by videoconference involving an accused person. In this case,

use of videoconference or another similar system in depositions and expert testimonies, as long as the mechanism at issue allows, literally: '*the bidirectional and simultaneous communication of the image and sound and the visual, auditory and verbal interaction…, assuring in any case the contradiction of the parties in litigations and the defence rights*'.

Especially, inside of the criminal jurisdiction, the employ of that technology is authorized during the judicial enquiry and during the examination of evidences for reasons of utility, security or public order (articles 325 and 731 bis LECrim., respectively),[23] but also as a mean of appear before the court of the Public Prosecutor during the judicial investigations (article 306 LECrim.).[24]

It is clear that the videoconference can be a determinant factor in order to save economic and human resources in the administration of justice. Even, it could be important to prevent unjustifiable delays

---

the decision to hold the videoconference, and the manner in which the videoconference shall be carried out, shall be subject to agreement between the Member States concerned, in accordance with their national law and relevant international instruments, including the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms.

Any Member State may, when giving its notification pursuant to Article 27(2), declare that it will not apply the first subparagraph. Such a declaration may be withdrawn at any time.

Hearings shall only be carried out with the consent of the accused person. Such rules as may prove to be necessary, with a view to the protection of the rights of accused persons, shall be adopted by the Council in a legally binding instrument'.

23 Both of them are literally the same, although the article 325 regulates the judicial investigation of the crimes and the second one the trial: 'El juez, de oficio o a instancia de parte, por razones de utilidad, seguridad o de orden público, así como en aquellos supuestos en que la comparecencia de quien haya de intervenir en cualquier tipo de procedimiento penal como imputado, testigo, perito, o en otra condición resulte particularmente gravosa o perjudicial, podrá acordar que la comparecencia se realice a través de videoconferencia u otro sistema similar que permita la comunicación bidireccional y simultánea de la imagen y el sonido, de acuerdo con lo dispuesto en el apartado 3 del artículo 229 de la Ley Orgánica del Poder Judicial'.

24 Literally: 'Cuando en los órganos judiciales existan los medios técnicos precisos, el fiscal podrá intervenir en las actuaciones de cualquier procedimiento penal, incluida la comparecencia del artículo 505, mediante videoconferencia u otro sistema similar que permita la comunicación bidireccional y simultánea de la imagen y el sonido [...]'.

in the procedures or the adjournment of a hearing. In this sense, it makes possible the performance of the judicial enquiry, still in long distances investigations, doing unnecessary that the courts have to come to other international or domestic assistance instruments, less respectful to the principle of immediacy. But also, on having avoided the need for displacement of individuals, it helps to limit the risks inherent in any transfer, specially recommended in case of dangerous pretrial inmates. For the Spanish Public Prosecutor, the possibility of save human resources is essential given the participation of this institution in each and every one of the jurisdictions.[25]

But, the advantages that we have emphasized should not turn the videoconference in the ordinary way to carry out the judicial investigation and, even less, to examine no real evidence. Besides to consider that justice has a ritual component that we must not eliminate, I realise that the physical attendance gives references such as the corporal language, which are not always faithfully reflected in the videoconference, system that, by its own nature, only allows a close up visualization of the individual, with a great expressive value. In addition, we must balance of the possible manipulation of the image that allows any audio-visual media, merely misusing the scene illumination.

For those reasons it seems recommendable that the enforcement of the rule respects strictly the exceptional nature of the cases legally covered.

6 Provisional conclusions: New times and new solutions

The technology offers opportunities until time recently unthinkable. The Justice Administration is adapting new

25 About those advantages see on the official website of Spanish Ministry of Justice (<www.mju.es>): Ministerio de Justicia [2007]. Also: Magro Servet (2005); Velasco Núñez (2002); Sevilla Gracia [2007].

technologies slowly, implementing some of these mechanisms to satisfy its own requirements. It would be stupid and counter-productive to be against to this phenomenon because the benefits that we can obtain seem evident and will almost certainly outweigh the disadvantages. For that reason I have subtitled my study 'Around a right road'.

But also we have to be aware that such new devices are merely assistive technologies and they will always have an instrumental nature.

Let me point out that Justice is something different from the other Public Administration and its goal cannot be merely to reach the highest levels of possible efficiency. I believe that Justice has an inherent human and ritual component. And those components have a meaning and are necessary also. Justice is not just a mechanical activity. I would venture to suggest that new technologies won't be the end of judges mindful of the proceedings, present depositions or appropriate treatment of inmates, sacrificing the human contact and the rituals for a supposed technical efficiency, or worst, just for economic reasons.

Finally, I must conclude that new technologies are one important aspect in order to improve the Administration of Justice as a whole, but obviously it is not the panacea to solve other normative or merely structural problems that there are to confront, such as an obsolete legal system, particularly in criminal jurisdiction, or the increase of litigation and the need of more human and material resources.

References

Cabezudo Rodríguez, N. (2004), 'Omisiones y recelos del legislador procesal ante los medios de prueba tecnológicos', *La Ley*, no. 6158 (30 December), pp. 1–5.

Cabezudo Rodríguez, N. (2006), 'Las nuevas tecnologías en las actuaciones judiciales', in Fernando Galindo Ayuda (coord.), *Gobierno, Derecho y Tecnología: Las actividades de los poderes públicos*, Pamplona: Thomson/Civitas, pp. 615–40.

Giménez Ontañón, V. (2003), 'Estado actual de la utilización de la videoconferencia en la Administración de Justicia', *La Ley*, no. 5831 (24 July) (<www.laley.es>).

Gómez Martínez, C., 'La grabación del sonido y la imagen en los juicios civiles. Del juez lector al juez espectador', <www.juecesdemocracia.es/publicaciones/revista/articulosinteres/lagrabaciondesonido.pdf> (visited 10 June 2007).

Gudín Rodríguez-Magariños, F. (2005), 'La cárcel electrónica. El modelo del derecho norteamericano', *La Ley Penal*, no. 21 (November), electronic version.

Iglesias Río, M. A., and J. A. Pérez Parente (2005), 'La pena de localización permanente y su seguimiento con medios de control electrónico', in *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, Burgos, Universidad de Burgos, Burgos, pp. 395–432.

Klein-Saffran, J., 'Electronic monitoring v. Halfway Houses. A study of Federal offenders', <http://www.bop.gov/news/research_projects/published_reports/gen_program_eval/orepralternatives.pdf> (visited 15 June 2007).

Magro Servet, V. (2005), 'Nuevas tecnologías en el proceso penal. En particular el uso de la videoconferencia', *Estudios de Derecho Judicial*, no. 58, pp. 176–205.

Ministerio de Justicia, *Sistema de Videoconferencia de la Administración de Justicia. (Plan de implantación del sistema de videoconferencia)*, <www.mju.es> (visited 15 June 2007).

Pedraz Penalva, E. (2003), 'Reflexiones sobre el procedimiento para el enjuiciamiento rápido de determinados delitos', *Revista Jurídica de Castilla y León*, no. 1, pp. 13–90.

Poza Cisneros, M.ª (2002), 'Las nuevas tecnologías en el ámbito penal', *Revista del Poder Judicial*, no. 65, pp. 59–134.

Sevilla Gracia, J. D., 'Nuevas tecnologías y arquitectura judicial', <http://www.cej.justicia.es/pdf/publicaciones/secretarios_judiciales/SECJUD70.pdf> (visited 21 July 2007).

Velasco Núñez, E. (2002), 'Videoconferencia y Administración de Justicia', *La Ley*, no. 5630 (10 October) (<www.laley.es>).

A SURVEY OF CIVIL AND CRIMINAL e-JUSTICE SUPPORT SYSTEMS IN ITALY

Cesare Maioli,[1] Giovanna de Rugeriis[2]

1 ICT and the Ministry of Justice

The ICT system at the Italian Ministry of Justice is managed by DGSIA (Direzione Generale dei Sistemi Informativi Automatizzati), a central office for automated information systems. This division is entrusted with developing and managing computer systems for all ministry offices, off-site administrative offices, and judicial offices. The ICT division is also responsible for interlinking all information systems within the Justice Ministry integrating these systems with those of outside government agencies, and for training the human resources needed to develop and use these ICT services.

1.1 Evolution over Time

The DGSIA division came into being with Legislative Decree No. 39 of 12 February 1993, which under Article 10 set up an authority called AIPA[3] (Autorità per l'Informatica nella Pubblica

1 CIRSFID and University of Bologna, Italy, <cesare.maioli@unibo.it>.

2 Ministry of Justice, Bologna, Italy, <giovanna.derugeriis@giustizia.it>. The authors worked jointly on this paper: Cesare Maioli wrote parts 1.2.1, 2.1, 2.2, 2.2.1, 3, 3.1, 4, 5, 5.1, and Giovanna de Rugeriis wrote parts 1, 1.1, 1.2, 1.2.2, 2, 2.2.2, 3.2, 5.2.

3 AIPA is the Italian authority entrusted with designing and developing ICT systems in government, overseeing this development, and coordinating ICT projects initiated at different government agencies. In 2003 it evolved in a new organization named CNIPA.

Amministrazione), and which requires that each ministry agency designate, without outsourcing, a general director entrusted with all ICT systems and with handling relations with AIPA, a role in which the general director is responsible as well for ensuring administrative performance under the ICT system he or she is in charge of.

The same decree, under Articles 16.1 and 16.8, calls for government regulations setting out the different ways in which the technology is to be used in administering justice.

The decree DPR No. 748 of 28 October 1994 (titled 'Applying LD No. 39 of 12 Feb. 1993 to the Administration of Justice') sets out under Article 1.2 the objectives to be pursued in the effort to administer justice by way of ICT tools: the use of content-management tools necessary for such administration.

Under Article 1(c) of this decree, the general ICT director to be appointed within each ministry agency pursuant to Article 10.1 of LD 39/1993 must be a magistrate.[4] Only in 2005 was this provision changed, to the effect that the person in charge of each agency's ICT system can either be a general director or a magistrate having equal competence as a general director.

Decree DPR No. 55 of 2 February 2001, titled 'Regulations for Organizing the Justice Ministry', reorganized the ministry by setting up four administrative and management departments, one of which is the Judicial Organization, Personnel, and Services Department, and it was within this department that the DGSIA was set up (pursuant to Article 6 of the same DPR).

---

4 A description of the organization of courts in Italy is in Intravaia (2006). It may be worth specifying that in Italian judicial system, under the term 'magistrate' is meant all the professionals who are judges or public prosecutors, with the same dignity and powers, training, recruitment rules, but different roles and functions in the trial and different offices of belonging; they can also change sector and move from a role to the other, with some restriction introduced by the recent law for the organization of the judicial power (Law no. 150/2005).

1.2 Internal Organization

Each general ICT director controls the budgets earmarked for developing and maintaining each ministry agency's information system. A meeting of ministry department heads can be convened jointly by the justice minister along with the general ICT director or with the heads of the departments having a direct stake in the issues at hand.

The DGSIA is headed by a general director and three magistrates responsible for the civil-law area, the criminal-law area, and the judicial-opinions area; it is staffed by 560 employees, among whom are 440 ICT experts, 120 administrative people, and 17 administration managers, 4 of whom under DGSIA and 13 under CISIA (Coordinamenti Interdistrettuali per i Sistemi Informativi Automatizzati: Inter-District Coordination for ICT Systems).

The structure of the DGSIA has been defined through a Justice Ministry decree issued on 18 December 2001. Under Article 8 of this decree, the DGSIA structure breaks down into 8 central offices and 13 territorial-coordination offices, these being the CISIA offices just mentioned, each of which has authority over one or more regions.

1.2.1 *The Offices Entrusted with Territorial ICT Coordination*

CISIA offices are responsible for managing ICT services and for coordinating central administration with outlying judicial offices across a given jurisdiction.[5] Specifically, this means that (under the provisions of DM 18 Dec. 2001) these offices must (a) identify the ICT needs of ministry offices across the territory, (b) manage the funds and tools necessary to meet these needs, (c) follow local projects and implement national projects on a territorial scale, (d) procure ICT services and equipment, (e) give opinions about the economic sustainability of suggested ICT solutions, (f) provide

5 A jurisdiction so understood as a geographic area under a single administration is otherwise often referred to as a 'territory'.

ministry offices with assistance and advice, and (g) handle relationships with CISIA district magistrates, with the administrative managers of ministry offices, and with external company and contractors providing services.

These tasks can be grouped under two broad areas, the one pertaining to the ICT themselves and the other to contracts, accounting, and bookkeeping. The ICT area is the very reason why CISIA offices have been set up in the first place, to be sure, but the contracts-and-bookkeeping area is no less important, this owing to the sheer quantity of work involved and to its role in making the primary CISIA activity functional and efficient.

A legislative decree was issued in 2006 (LD No. 240 of 25 July 2006) which regulated the tasks and authority of the area judges under DGSIA, of the administrative managers, and of the ministry offices, and which also made provision for decentralizing some ministry functions to the regional governments, pursuant to Articles 1.1(a), 2.1(s)(t), and 12 of Law No. 150 of 25 July 2005. As part of this scheme, certain regional and interregional administrative offices are to be set up which will be responsible for ICT systems, among other things.

This decentralized framework will clearly make it necessary to reorganize CISIA offices as they are currently operating, so much so that under Article 11 of the same LD 240/2006 regulating the transition period, the regional administrative offices will be set up at CISIA locations while the decentralization process is still underway. Likewise, Article 9 provides that the regional administrative offices be staffed by drawing in the first instance on the personnel already at work to run CISIA offices.

1.2.2 *The District Magistrates Responsible for Ministry ICT Systems*

When it came to implementing LD 39/1993 at the Ministry of Justice – by entrusting people with ICT systems at different districts – the Consiglio Superiore della Magistratura (CSM) resolved that

this role should filled by the district magistrate responsible for ICT systems, and that the appointment should be made by CSM itself by selection on the basis of a competition. This was established by way of a CSM resolution of 26 Jan. 1995, which, in line with the dual scheme in place at other justice agencies, set up a system for the governance of ICT under which the magistracy operates in autonomy in parallel with administrative personnel.

The CSM found that justice offices suffered from a lack coordination with the central administration at the Ministry of Justice, and it was with this end in view that this solution was found, namely, having for each district one or more district magistrates supported by administrative managers.

Circular Letter No. 15849 of 10 Nov. 1995 later specified in some detail (a) the role of the district magistrates for ICT systems, as well as (b) their status and (c) their relationship to other ministry officials in the territory:

(a) Their general role is to offer the technical support the ministry needs in its effort to provide service to administer justice through the use of ICT; specifically, this means that district magistrates have to assess the ICT systems within their districts and carry out on this basis initiatives and projects aimed at making sure that these ICT systems are functional to the need to achieve coordination among ministry offices.

(b) The status of district magistrates is defined in certain tables laying out the personnel structure under the country's courts of appeals,[6] and it has been established that magistrates serving in this role should be relieved of judiciary workload in proportion to the time and effort they devote to ICT coordination.

(c) Having conducted a comprehensive nationwide assessment of the activity carried out by the ICT district magistrates, CSM thus

6 The tables in question are a matter of administrative regulation. They are issued every two years and establish the organization of each judicial office with a view to facilitating coordination and specialization.

decided (two years into the program) that their role should be reframed. In its report, CSM found that the initial start-up work had been completed – the Ministry offices having been networked under a single system, and the procurement of software and hardware equipment no longer placing a heavy burden on the ministry itself (this thanks to certain CONSIP agreements) – so it made sense at that point for ICT district magistrates to devote themselves to less technical tasks more suited to the role initially ascribed to them as liaisons between the judicial function and administrative work.

The role of the district magistrates responsible for ICT systems was accordingly redefined, by entrusting them with five main tasks as follows:

(i) encouraging colleagues to appreciate the innovation involved in using ICT tools for the administration of justice, and helping them acquire the skills and knowledge necessary to this end, especially in environments where time is scarce;

(ii) analyzing the software used in the administration of justice, with a view to making it easier to take part in processes by which 'legal-process products' are created;

(iii) playing a part in testing the software applications in actual use, so as to provide a link between the applications' user base and the Ministry of Justice;

(iv) using the technology for trial procedure, so as to make workflow more fluid for the entire cast of characters involved in a trial (i.e., judges, lawyer, court reporter, and anyone using the ministry's services);

(v) making sure that the technological solutions adopted are appropriate, so that all outlying offices can work under standard procedures consistent with those of the central administration.

The Italian justice system is bringing the ICT into wider and wider use, in the civil and the criminal process alike, which are developing in parallel yet in ways distinctive to each. Indeed, while both processes share a set of objectives and methods – i.e., efficient

judicial and administrative action under a single overall procedural framework – they part ways when it comes to the laws and regulations that each process deals with and the roles of those involved in each process, and this bifurcation must therefore be reflected in the relative ICT systems.

The separation is maintained even by the governance bodies entrusted with the ICT administration of justice. In fact, the general director at DGSIA is supported by two area magistrates responsible for the civil and the criminal process respectively, and the ICT district magistrates are likewise responsible for separate civil and criminal areas.

2 ICT in the Administration of Civil Justice

The first area of office work to have been automated at the judicial offices was court records: these are the main repositories of judicial information, and the data they carry (such as record number, partition, subject matter of the case, and status of the proceeding) makes it possible to monitor the lifecycle of the proceeding itself and easily manage the relative paperwork. In other words, these are transaction-processing systems that record the daily routine work an office performs to administer justice.

Under Ministry of Justice Decree No. 264 of 27 March 2000, on record-keeping regulations for judicial offices, these offices are required to keep digital records whenever DGSIA-certified software applications are available. Before that time (under a decree issued on 9 November 1989 by Minister Vassalli),[7] the rule was that digital records could replace paper ones as long as the two were consistent. Decree No. 264/2000 reversed that priority, making the digital record the default standard, all the while enabling the paper form to stand in, but only for compelling reasons obtaining in exceptional cases.

---

7 D. Intravaia, 'Il processo civile telematico' [The Online Civil Process], in M. Jori (ed.), *Elements of ITC Law*, Milan: Giappichelli, 2006.

Decree No. 264/2000 has been integrated by a ministry decree issued on 24 May 2001, titled 'Procedural Rules for Keeping Digital Records in the Administration of Justice,' serving as the basic user's manual for all the software applications used at the ministry to replace the paper trail.

These procedural rules closed the project phase in which software was being developed locally (which is still possible to date, but only in certain limited cases and never without with DGSIA authorization). Now a new phase is under way, the national phase, in which applications made to last over time are being released centrally by DGSIA where local tweaking and customization receive increasing attention.

The record-keeping applications make it possible to manage information over time and are based on a state-event paradigm: at date 1 the procedure finds itself at state 1 (e.g., a hearing has been held pursuant to Article 180 of the Code of Civil Procedure, or CCP); then event a takes place (e.g., the trial is adjourned to a later date) and the process passes into state 2, scheduled to take place on date 2 (e.g., another hearing is held pursuant to Article 183 CCP).

2.1 Information Systems for Processing Transactions

Information systems for processing transactions under the civil process divide into three types: (a) systems for the judicial proceeding (includes all evidence, testimony, pleadings, etc.); (b) systems for judgments and court orders (when a judgment is rendered and enforced or a court order carried out); (c) systems for small-claims courts before a justice of the peace.

(a) The main systems for the Judicial Proceeding are:

(1) Information System for Civil Litigation (SICC). This system, completed in 2001, is designed to manage court records throughout the course of a trial from the initial complaint filed with the court to the time when the parties each rest their case, thus making it possible to coherently organize all information pertaining to the proceeding

and send it out to the appropriate records office (these being divided by type into 'Role', 'Subject' and 'Object').

(2) Information System for Employment and Labour Law (SIL), with schemes and functions similar to those used for ordinary proceedings.

(3) Information System for Probate and Non-Contentious Jurisdiction (SIVG). This is a system for all matters resolved outside the context of litigation.

Transaction-processing systems for ordinary judicial proceedings are in use at 90 percent of all first-tier and second-tier judicial offices, which means a total of about 180 offices. Currently in process, too, is a Web application called SICID which will serve jurisdictions at district level and which will merge onto a single platform the three separate applications now in use for ordinary judicial proceedings.

(b) The main systems Judgments and Court Orders are:

(1) Information System for Civil Judgments (SIEC). This system automates judgment relative to movable and immovable property.

(2) Information System for Automating Bankruptcy and Insolvency Proceedings (APC). This is still a pilot project being tested at selected locations and will make it possible to manage adjudication, liquidation, receivership, and composition, among other things.

Information systems for judgments and court orders are in use at 25 percent of all the judicial offices that are due to phase them in, which means a total of 160 courts. Here, too, a single application is being developed, called SIECIC and designed to make the two systems Web-based at district level.

(c) Information System for Small-Claims Courts before Justices of the Peace consists of a single system called SIGP. Its basis was a prior system that has been reengineered using district-level Web architecture and has been made interoperable with Polis Web. The system is in use at 25 percent of all small-claims offices (800 of them nationwide), and that figure jumps to 60 percent when we take only the larger offices into account.

2.2 Decision Support Systems and Online Civil Trial

A decision-support system called Polis has been created which makes it possible to draft and look up rulings and build databases collecting the case law of local trial and appellate courts, thus providing magistrates and lawyers with support in arguing cases and rendering decisions. The Polis system can be used to compile, publish, archive, and index all the legal documentation produced within a court of law. It was developed in the 1990s yet has until recently been little used among magistrates.

Polis is part of an effort to implement so-called Online Civil Trials (OCT), and it now forms part of what is known as the Judge's Console, a system that makes it possible to manage the judge's calendar and work by pooling together all the digital records maintained by a court and retrieving from these records all the information necessary to try cases and issue orders and decisions. The console can be used to manage the single judicial proceeding or the judge's activity at large. Its components are a date-book, an editor (for drafting legal opinions and other judicial documents), and a number of tools for querying and analyzing case law.

2.2.1 *Remote Access to Legal Documents*

PolisWeb for lawyers is an Internet and Intranet site built by the Italian Ministry of Justice (launched on 10 December 2004) enabling personalized networked cooperation between judicial offices and lawyers, who can use the site to access all data stored at these offices. PolisWeb is supported by Polis system along with SICC, SIL, SIVG, and SIEC. Authorized users can view documents, gain online access to information relating to the proceedings they are following, and go online to place requests for copies of rulings.

Users access the system by launching a standard Web browsers and authenticating themselves through a cryptography device (typically a smart card) from an access point external to the Ministry of Justice domain. The PolisWeb site is hosted by CG_Amm (Naples), the justice agency charged with maintaining all services for interoperability

between the ministry itself and the Internet at large. The service can also be used locally from within ministry locations: the system is called PolisWeb Intranet, which gives access to content by way of a local server.

2.2.2 *The Online Civil Trial*

The Online Civil Trial (OCT), first developed in early 2000, is a broad project that brings together all the other systems so far described and takes them to their next logical step.

The idea is to have a unified information system by which to create and update digital files, understood as sets of digital documents structured so as to make it possible to track changes over time.

The system supports the civil process by enabling users to log onto the Internet to carry out operations such as filing legal instruments with the court, sending notices and communications, checking the progress of judicial proceedings, viewing documents stored at the records office, and accessing case law. This means, in short, that ICT tools can be used to carry out all proceedings except for hearings, which for the time being is still regarded as requiring the participation of people in flesh and blood.

A great deal of effort went into setting up a controlled, reliable, and secure environment, by way of such devices as certified mail, smart-card identification, digital signature, and data cryptography. All documents are exchanged in XML format, so as to enable automatic population of the archives maintained by the records offices.

The system is accessed from an access point external to the Ministry of Justice domain. The access point is managed by ministry-certified professionals (such as lawyer orders) and makes it possible to manage user authentication. Also forming part of the system is a central nationwide management office, based in Naples and internal to the ministry domain, entrusted with managing transactions with all authorized users and keeping track of access dates and times. When a transaction is completed, the records office acknowledges this by way of a digitally signed return receipt sent to the user at his or her access point.

OCT are currently in use at the Milan Tribunal (as from 11 Dec. 2006) and only for summary judgments. The plan is to expand OCT, by way of standardized ICT tools, and to apply them as well to social-security claims and proceedings (in which one of the parties to the transaction is a government agency such as INPS, INPDAP, or INAIL) and to mortgages and foreclosures (in which one of the parties is a credit institution). In a step closer to this latter objective, the Ministry of Justice signed an agreement on 22 Nov. 2006 with the Italian Association of Banks (ABI).

Still, OCT are still in their infancy. The Italian government hopes to use them to make the administration of civil justice more efficient, and in view of this objective it has submitted to Parliament a draft law (better known as the Mastella DDL)[8] making OCT mandatory at all judicial offices by the year 2010.

It is expected that this will speed up judicial proceedings (especially by making it easier to process formal requirements needed carry on with the trial and proceed to a final judgment), and a further advantage expected to come out of OCT is that of expanding the knowledge base by improving content access and management once documents are digitized, structured, and collected into databases, thereby also making for better management of resources generally.

The Mastella DDL, if passed, would make OCT mandatory at all Ministry of Justice offices by the year 2010. Article 6.2 of this DDL provides, too, that any judicial district may move this deadline back to an earlier date by way of a Ministry of Justice decree, but only on the condition of first hearing the opinion of the lawyers' association operating in the district at issue, and so long as the relevant judicial offices have the necessary equipment. The proposed law also limits the initiative to areas of the law concerning summary judgments, foreclosures and mortgages, and social-welfare claims.

---

8 Mastella is the name of the minister; DDL stands for *disegno di legge*, meaning a draft law.

A clear signal of the political will to make the Italian judicial system more efficient by bringing information technology into wider use within the system comes from the Ministry of Justice, which has conducted an OCT feasibility study and has set a deadline for implementing OCT. Should the Mastella DDL earn parliamentary approval, the task of streamlining the civil process with respect to those areas singled out in the DDL itself fall to the public administrations concerned. An innovative feature of the DDL, as currently framed under Article 6.1, is that the judiciary's administrations are required to use the full potential of ICT in the effort to administer justice in the most cost-effective and functional way.

Yet the main innovation introduced by this DDL lies elsewhere. So far, the OCT has been developed within the framework of the rules of civil procedure (as set forth in the Code on Civil Procedure and in other statutory provisions), the idea being to achieve compliance with these rules without changing the rules themselves, that is, without reengineering the procedure itself. In fact, ICT are meant to serve as support in processing activities instrumental to the parties' ability to assert claims (activities such as notices and communications to be served, which play an essential role in guaranteeing the parties' rights within the trial, such as the right to initiate an action and the right to confrontation), and it has long been the assumption that by relying on ICT to process these activities we would risk undermining procedural due-process guarantees in such a way that the parties to the suit would get unequal treatment. In reality, ICT can help us both normalize and speed up judicial proceedings, in that swift action in protecting the parties' interests does not thereby entail loosening up the standard of certainty in law (in fact the two go hand in hand). For this reason, the Mastella DDL introduces a welcome innovation if it provides that procedural rules can and should be reframed so as to make them functional to the online trial itself, in the name of efficiency.

This development marks a turning point, we believe: it is revolutionary if we consider how it can be used to great effect in bringing ICT into wide use in the civil process. Presumably, other

like-minded initiatives will follow in the criminal process, which requires stronger guarantees.

Then, too, making it possible to reframe criminal procedure so as to render it functional to the online trial does not necessarily entail relaxing procedural guarantees – not if the technological means used are reliable. Thus, for example, we will have to use[9] certified e-mails and digital signatures (mandatory for judicial offices, attorneys, and judges and assistant judges; on request for all the parties to a criminal suit, including witnesses): these tools will have to enable us to ensure that all communications are authentic, whole, and final (non repudiation of communication).

The rules and subject areas that will have to be revisited in the effort to make for an efficient online trial are not inconsequential. They include notices and communications to the parties and the court, assignment or appointment defence attorneys (under power-of-attorney rules), the role of judiciary officials in serving notices, the forced sale of movable goods, and the payment of trial costs (Article 7 of the Mastella DDL). Simplifying the service of notices will involve striking formal requirements out of the procedure, but in such a way that the parties retain all the guarantees afforded to them under the law, and so that the focus of these notices will shift to the defendant as the main or sole addressee.

Under Article 8 DDL, all filing of court rulings and judicial remedies and orders in civil matters with the national revenue service (Agency for the tax money Collection) will have to take place digitally over the Internet. The same goes for payments of social-welfare withholdings and of the expenses associated with the civil process: under Article 11 DDL, these payments will have to be made by wire transfer going through either a banking or a postal service, and may also go through credit or debit cards or other form of electronic funds transfer. This will entail a coordination effort between the Ministry of Justice and the Finance Ministry.

---

9 Legislative decree 7 March 2005, no. 82, known as 'Code of digital administration' updated by Legislative decree no. 159, 4 April 2006.

Similarly, Article 10 DDL encourages use of digital copies of documents by placing a 50-percent cost increase on requests for paper copies of documents issued by the judicial offices.

To be sure, this DDL may never be written into law, or it may pass in a different form, but even then, it is significant enough that we have a formal statement expressing this basic idea about the ICT, namely: that if we are to use these technologies to good effect in the judicial process, we will first have to simplify the process itself (its rules and procedures), and in a way that makes sense with respect to the project of implementing an e-Justice system.

There is reason to be optimistic in this regard, because the transition – toward a streamlined, more practical procedure – has already been effected at other government agencies and institutions, and now the justice system is beginning to do the same as well.

3 ICT in the Administration of Criminal Justice

The aforementioned Ministry Decree No. 264/2000, requiring that office registries be computer-based by default, proved instrumental in the subsequent effort to introduce integrated data-interchange systems.

It is essential for judicial offices and external judicial agencies to be able to exchange data. Interaction among different systems is paramount, since procedures require different interfaces with different subjects and institutions to maintain a constant line of communication. This makes for greater complexity in deploying ICT tools, since communication flows need to be rationalized and standardized.

The criminal-justice system has automated registries and implemented numerous information systems to support investigation mainly of organized crime. A challenge now is to develop information systems for support in the various phases of a criminal trial, so as to have a fully interconnected system.

The situation is similar in juvenile and correctional justice, where procedures require cooperation with different agencies (including welfare) from which to obtain information.

There are four main objectives for 2007 to 2009:

(1) to concentrate ICT servers at district level;

(2) to move toward Web-based applications for the information systems used in handling (a) jurisdiction, (b) sentencing and enforcement, and (c) crime prevention;

(3) to expand cooperation and interoperability systems;

(4) to improve the systems in use.

Here focus is on objectives (2) and (3), since (1) is mainly technological and (4) mainly logistical and so are instrumental.

3.1 Evolution of Information Systems

Jurisdiction management is mainly based on two information systems:

(a) REGE aims at the management of general registries, an automated version of the criminal registry used by trial courts. First implemented in 1989 with the new Criminal Procedure Code, the system has since been evolving through more sophisticated database management and Web technology. It manages the criminal register from the first notice of a crime to the first sentence, and it stores information about the crime and the people involved. The system can also be used to automatically extract the statistical crime data and to enable information exchange between the prosecutor's office and the court.

(b) NSC (literally, Nuovo Sistema informativo del Casellario giudiziale, i.e., New Information System for the Records Office). The effort to automate judicial record-keeping has recently made headway with implementation, in 2007, of an ICT data-entry and management system for data relative to any court-issued provision, enabling the issuing office to accurately enter the information through a user-friendly interface developed in a Web environment. The NSC system

was brought into operation pursuant to DPR No. 313 of 14 November 2002, a consolidated text laying out the statutory requirements and rules the records office must operate by. But the NSC does not fulfil the whole of the DPR: indeed, this DPR sets out data-entry procedures for the records office and the office for crime-dependent administrative penalties, and these procedures are already operational, but there has yet to be a database for verifying the caseload of criminal cases on the national docket. This will happen under the national ICT plan for the three-year period from 2007 to 2009, which calls for a project for automatically feeding the records office with the data stored in the so-called source systems (e.g. REGE).

Sentencing and enforcement are managed by way of two main information systems as follows:

(a) An automated registry of criminal sentences for magistrates supervising the execution of monetary fines and other criminal punishments.

(b) An automated enforcement system for magistrates supervising the execution of prison sentences and alternative measures. The system can be used to draft documents and build databases collecting information on people seeking reduced penalties.

Crime prevention breaks down into two areas:

(a) Precautionary measures. These include preventive detention and are designed to guard against misconduct awaiting judgment; their term is limited and expires regardless of how long the relative investigation and proceeding might last. A system is therefore being developed to manage the information relating to a proceeding as it unfolds, with a database of court-issued precautionary measures making it possible to monitor expiration dates on these measures.

(b) Seizure and confiscation. This relates to goods and property confiscated from organized crime and used for a public purpose, as provided for under Italian law. The system will make it possible to automate data retrieval, enabling law enforcement to exchange data with the Finance Ministry, which is entrusted with ensuring that confiscated goods are actually put to a public use.

3.2 Systems Integration and Interoperability

Several information systems benefit from cooperation between investigative bodies, judiciary offices, and external and international organizations.

Two such systems are SIDDA and SIDNA, supporting investigation by the National Anti-Mafia Office (DNA) and the District Anti-Mafia Offices (DDA). These systems are designed as information services based on a central repository that organizes data collected by local offices and makes it possible to exchange information relating to trials against organized crime. Secure communication is guaranteed through proprietary software enabling data encryption and security checks across a unitary justice network. The repository stores multimedia data such as texts, images, and video and audio recordings (from wiretapping). Under special conditions, the database may be accessed by judicial police too.

Local DDA offices can only access their own data, while the national coordinating office (DNA) has access to all information on file.

The information systems supporting international cooperation between the judiciary and prosecuting offices are:

(a) A system supporting investigative groups cooperating under Eurojust. This is a DGSIA information system helping prosecutors in different EU member states carry out investigations and coordinate under Eurojust. Different prosecutors and groups investigating the same case can use the system to collect, find, retrieve, exchange, compare, and analyze investigative data. The technology is the same as in SIDDA and SIDNA.

(b) e-Court. This (partly EU-funded) system helps criminal courts across the EU cooperate by sharing integrated multimedia data. The ICT technology includes 'intelligent' information retrieval with document indexing, thesaurus refinement, and multilingual searching.

(c) A criminal-data management system based on cooperation between the Justice and Interior Ministries. The system enables the criminal investigative units of the Interior Ministry to centralize their

data and relay it to the Justice Ministry, which in turn forwards it to the relevant prosecuting offices so that they can update their automated REGE registries. This is expected to bring a number of benefits: (i) criminal offices will work more efficiently through access to constantly updated REGE data; (ii) backlogs and errors owed to misreading of paper documents or incorrect data entry will be reduced to a minimum; (iii) law-enforcement institution receiving updated information about a crime will be able to give feedback.

Further significant operation systems are:

(a) Minerv@ system that helps public prosecutors to simplify routine activities (such as launching an investigation) and do advanced management of criminal dossiers.

(b) TRIN (Intelligent Court) system that enables multimedia management of hearings, with additional tools for audio and video recording serving to integrate the transcript tools already available at the court.

4 An Evaluation Model

The ICT are being phased into the Italian justice system along models similar to those of other European systems. Specifically, we have seen a three-phase pattern[10] whereby (1) ICT expand their presence, (2) ICT help improve governance, and (3) their impact is evaluated on the basis of shared quantitative data and user satisfaction.

(1) ICT systems were first introduced in the 1980s, with basic tools for automating administrative office work, simple audio equipment in the courtroom, and collections of law on CD-ROM and centralized databases. Then cases were being managed through the ICT, but only locally and often without knowledge sharing: REGE started this way in the early 1990s.

10 Contini (2001).

Entire office suites then came into use, along with a few systems for managing dockets: they were sporadic initiatives, based on an uncoordinated 'Act first, think later' approach, but then as the benefits became apparent, the ICT started winning more acceptance and replacing a system overwhelmingly based on the paper shuffle. In parallel, it became clear that any further growth in the same direction was going to require a restructuring the justice system through planning and training.

(2) In the second phase, governance bodies were thus established – such as AIPA for the public sector and DGSIA for the justice system – which worked to coordinate the early initiatives with two related goals uppermost in mind: expanding these projects and giving them a strong footing.

For the first goal, AIPA combined skills and expertise in the ICT with an ability to work out the relations among the different participants in the justice system, that is, law enforcement, the bar and bench, the ministry, CSM – all of whom had different goals, values, workloads, and procedures.

The second goal was pursued by drawing judges and prosecutors into the very design process of developing ICT solutions for the administration of justice, all the while bringing in ICT experts and consultants: this made it possible to overcome the traditional 'make or buy' alternative and have tailored systems whose use judges and prosecutors could easily master.

This second phase[11] led to a number of improvements: integrated office and case-management systems, more statistical data on which basis to assess performance, automated transcription of hearings and e-Filing of documents, and a greater use of open networks to administer justice (as through intranet systems) and offer consultancy (as through PolisWeb).

(3) In the third phase, presently underway, the whole e-Justice system has become of focus of policy (with the Mastella DDL, for example)

11 Contini (2001).

aimed at further integrating its different components and procedures, to this end laying greater emphasis on Web technologies.

The problem is especially felt in criminal justice, whose different participants (e.g., police and probation officers, prison guards, prosecutors, and courts) operate by markedly different methods and procedures. The effort is therefore to standardize operations as must as practicable, thus taking full advantage of tools such as digitally signed documents and certified e-mail.

5 Conclusions

The main problem is in the inherent characteristics of the organizational structure of the personnel belonging to the justice sector who are supposed to plan and coordinate the use of information systems: the DGSIA is an organized entity with clearly defined hierarchical department structure, proper plans, reporting rules, and productivity standards to achieve; the DGSIA personnel conforms their behaviour and performance to managerial performances and administrative standards, topics quite separated from the jurisdictional functions.

On a different side the magistrates are mainly and duly concerned with administering justice and prosecuting crimes, with a large independence of behaviour guaranteed by a long tradition and by the Constitution. Thus there is not, for magistrates, the possibility to represent and manage their activities as the ones a business or a service company are used to, with regard to use information system based on ICT.

The way in which digital documents are used and managed is fundamentally different from the way magistrates have always been accustomed to conceiving of the document itself: no longer is it immediately clear which is the copy and which the original, for example, or what is to count as distribution or communication – and this forces magistrates to make assessments and decisions requiring a different kind of expertise, and involving document-production processes over which they can exercise no control.

In our opinion, the vision to pursue is to structure the administrative department in a way as to isolate a group of non magistrate personnel, on the example of court managers in the US, who is in charge of case-flow management, filing and e-Filing, provisions and management of the ITC systems whose main users are the magistrates.

5.1 Development Methods

As we have seen, e-Justice combines organization, technology, and law, and for this reason a corresponding process analysis has been developed that takes these different aspects into account. The method – adapted from Business Process Reengineering (BPR)[12] – accordingly involves (i) describing the range and purpose of the services provided; (ii) analyzing how information flows through the system and what function this serves (an as-is analysis); and (iii) remodelling such as-is functions and practices in light of the purposes described and of applicable law (so as to achieve compliance).

The initial assessment is carried out in the course of meetings with the people running the organizational units and with practitioners in the field.

Then came the actual reengineering stage, which took two basic criteria as its guide, the whole point being to model processes that are both (a) efficient and (b) compliant with the law.

Thus, in the first place, administrative procedures have been redefined on the basis of the BPR plan, and corresponding changes were singled out for integration into the ICT system. The big challenge here is usually to make the entire process seamless and consistent: in practice there are clumsy processes both fragmented and largely paper-based, with procedure broken up into many pieces, with documents being stored in separate archives, sometimes digital, other times

12 The BPR method was first developed in the 1990s by M. Hammer, *The Reengineering Revolution*, New York: Harper Collins, 1995.

conventional and it is often difficult to find any single person in charge of an entire procedure and capable of carrying it through. So part of the effort has been to translate paper procedures into digital ones, and another focus was on making for secure access to procedures.

But at the same time, the procedures and micro-processes themselves needed to be brought into line with statutory requirements and be framed for administrative transparency. All judicial services relative to the civil and the criminal process had to be made compliant with the law, and especially with the rules concerning administrative procedure, document digitizing, and privacy.

For what concerns the way the DGSIA and the Justice Ministry approached system development, some users and researchers dislike the hierarchical top-down approach on which ICT systems have been designed for the justice sector: we disagree with this line of criticism.

Neither the top-down nor the bottom-up approach is inherently superior to the other. Generally, top-down is thought to require more experience and maturity on the part of both analyst and user; it is also considered less time-consuming, since experienced personnel tend to work top-down and find this approach easier for transaction processing and more difficult for decision-support systems.

But top-down works better when development is being led by an institution entrusted with organization, to this end collaborating with an institution entrusted with ITC (here DGSIA), thus sharing the same set of objectives for the information systems being developed.

Moreover, breaking problems down into more-elementary terms encourages solutions arrived at by stepwise refinement, making it possible to fine-tune the system with ever subtler distinctions and nuanced components closely adapted to the purpose.

Justice is administratively organized in a strictly hierarchical way, so in this case top-down seems the best approach, for it makes it possible to achieve a seamless system as development moves ahead

from one stage to the next,[13] thus connecting (1) general policy guidelines, (2) an integrated plan combining organization with an ICT platforms, (3) detailed studies for each business process, so that ICT tools can be effectively integrated into processes and functions, and (4) database design whereby the phases singled out in process analysis can be accurately matched to the ICT tools used for implementing the same phases.

Particularly with respect to points (2) and (3) above, the key to success is feedback, which indeed seems to have been the idea in the pilot experiments carried out at courts of law in different cities across Italy, especially over the last three years. Systems for the administration of justice have been developed accordingly, using development techniques based on the idea of bringing the user into the process, techniques such as user-centred design[14] and participatory design.[15]

e-Justice is being fashioned after the e-Government models that Europe has been adopting since 1995 for many government functions. There is no reason not to develop e-Justice in keeping with the guidelines adopted for e-Government in general (as has been happening in e-Administration, e-Commerce, e-Banking, and e-Health). The principles involved may be summarized as follows:[16]

---

13 This view is strongly supported in the literature on information systems: see, for example, the seminal works of H. Simon, *Models of Thought*, Yale: Yale University Press, 1979; M. L. Gillenson and R. Goldberg, *Strategic Planning Systems Analysis & Database Design: The Continuous Flow Approach*, New York: John Wiley and Sons, 1984; and P. O. Flaatten et al., *Foundations of Business Systems*, Orlando, FL: Course Technology, 1989.

14 User-centred design emerged around 1985 as one of the most compelling criteria for developing user interaction. Its point is to frame interaction from the user's point of view rather than that of the ICT system. Effective user interaction requires focusing on what is best for the user, rather than on what is fastest and easiest for the developer.

15 User involvement can hep designers understand what tasks users need to perform, as well as how often they need to perform them and under what conditions. Working with users representing each of the relevant classes (district magistrates responsible for Ministry ICT systems, administrative heads, office clerks) can provide invaluable input giving insight into how the design may be improved.

16 R. Traunmuller and K. Lenk, *Electronic Government: First International Conference*, Berlin: Springer, 2002.

(1) A holistic view. This means that e-Government must proceed on the basis of an integrated view: it must seek to achieve a permanent transformation enabling governance on a comprehensive scale. (2) Service provision as focus. ICT services for businesses, citizens, and communities must be designed so as to serve needs as they emerge from outside government itself. (3) Redefining governmental processes. This requires thoroughly rethinking the machinery of government, so as to bring out many more situations in which ICT as an enabling tool can enhance the effectiveness, quality, and efficiency of public action, all the while making it more legitimate. (4) Knowledge-enhanced government. This requires shifting the focus from structures and processes to content, so as to get to the very heart of administrative work: the deeper the understanding of the connections between processes and knowledge, the better the resulting system design. (5) A sound engineering approach. This means that tools and methods for reengineering public-governance processes and institutions should take into account the role of human activity, knowledge, and decision-making capacities. (6) Reference models and administrative standards. Model practices and pilot projects should be used, because this will give an idea of the full potential. (7) Change management. Good government needs strong innovation, and the way to do achieve this is to look to the landmark projects as a guide, using the best practices and guidelines worked out on that basis rather than on new experimentation with peculiar approaches.

Developers working on e-Justice systems in Italy have clearly taken most of these principles into account. So, too, points (3), (5), and (7) in particular strongly suggest adopting a top-down approach.

5.2 A Guiding Vision and a Few Dangers

In agreement with a thought attributed to C. G. Jung, we think the great problems of humanity have never been solved by formal laws but can only be solved by working to refashion the underlying attitudes of those concerned – in our case, the management attitude and style of judiciary offices. This suggests that using the following guidelines will bring about virtuous cycle:

(1) making the ICT the standard working familiar to all persons and organizations;

(2) framing legislation and organization in such a way that different people and institutions can access and exchange content online and work out new shared procedures and products;

(3) encouraging personal and institutional use of such products and procedures, not only because they are legally established but also because using them builds a proactive attitude and an appreciation of their value;

(4) encouraging professionals and practitioners throughout the justice system to welcome new redefined roles and working methods, a redefinition that is ultimately inevitable.

Some of the challenges confronting the justice system are those attendant on any complex government function carried out on a broad scale. But there are also challenges specific to justice alone, chief among them a cultural undercurrent that is slowing down efforts to reorganize offices and redesign procedures in ways consistent with ICT projects however conceived (including projects based on any kind of BPR method). This has made it so that ICT projects for the administration of justice are often slow in coming and their results below expectation.

There have been training programs designed to teach proper use of the information systems designed for the administration of justice, but these systems are in many cases still being used inefficiently, and the data is being entered incorrectly, which not only brings down the quality of such data but also engenders scepticism about whether ICT systems can really be used to good effect in reorganizing justice.

ICT systems need a steady and durable inflow of financial resources if they are to do any good, but these resources have not always been forthcoming in the past.

A parallel problem is human resources, with government in Italy finding it generally difficult to keep qualified professionals on the public job, and the DGSIA has similarly been affected. This is a concern across the entire public sector, and it is cause for worry considering how hard it is to fill vacancies with qualified recruits.

References

Augusto, A. (2003), 'Judicial Electronic Data Interchange in Italy', in M. Fabri and F. Contini (eds.), *Judicial Electronic Data Interchange in Europe*, Bologna: Lo Scarabeo.

Borsari, G., 'Online Civil Trial', e-Gov Interop'05 Conference, Geneva 2005, <http://egovinterop.eupm.net/cdrom/pages/presentations/> (visited 7 July 2007).

Brescia, S. (2003), 'Report on the Online Civil Trial', in *Third annual report on the excessive length of judicial proceedings in Italy for 2003*, Strasbourg: Council of Europe.

Carnevali, D., and M. C. Di Cocco (2001), 'An Innovation Process Embedded in a Strict Institutional Setting: ICT in the Italian Judicial System', in M. Fabri and F. Contini (eds.), *Justice and Technology in Europe: How ICT is Changing the Judicial Business*, Amsterdam: Kluwer.

Contin, F. (2001), 'Dynamics of ICT Diffusion in European Judicial Systems', in M. Fabri and F. Contini (eds.), *Justice and Technology in Europe: How ICT is Changing the Judicial Business*, Amsterdam: Kluwer.

Fabri, M. (2006), *Administration of the Justice System*, Bologna: Clueb. (In Italian.)

Freiheit, D., et al. (2007), *Current state of the use of information technology within the justice sector in Europe*, Merzig: EDV-Akademie des Rechts. (In German.)

Intravaia, D. (2006), 'Status and Training of Court Administrators in Italy', in *Status and Training of Court Administrators in Albania*, Tirana: Ministry of Justice.

Nunziata, C. (2004), 'The crisis of criminal trial', *La Voce*, <http://www.lavoce.info/> (visited 7 July 2007). (In Italian.)

Rolleri, F. (2003), 'Conclusions', in *Internet Strategies and E-Justice in Europe*, Roma: Ministry of Justice.

e-JUSTICE IN BULGARIA

Bogdan Petrov[1]

1 The notion of e-Justice

e-Justice can be defined as any service providing information in electronic format related to a process in the Judiciary or, more generally, as the whole body of electronic exchange of judiciary information via telecommunications networks.

Examples of e-Justice applications include Internet-based services providing information to the public or supporting data exchange between citizens and judiciary organizations; services for information exchange between organizations; services supporting procedures within an organization (e.g. workflow systems); services supporting 'legal communications' (e.g. secure e-mail services implementing digital signatures); and services for digital audio and video communications (e.g. systems recording or/and broadcasting court hearings, remote surveillance and remote interrogation systems).

2 The Strategy

The strategy for introducing e-Justice in Bulgaria rests on three pillars:

— Legal framework (i.e. rules forming legal basis for each service provided);

---

1 Center for the Law of ICT (CLICT), 39 Shesti Septemvri St., Sofia 1000, Bulgaria, <bogdan.petrov@clict.net>.

— Technical arrangements (architecture, infrastructure, applied technologies, etc.);
— Operation plans (manpower, training, maintenance, procedures, etc.).

The principles the strategy is based upon are:

— Transparency: enhancing visibility in justice and public administration, strengthening trust between the Judiciary and the public;
— Accessibility: allowing people to access fast and reliably the information they need;
— Usability: providing tools that are useful and easy-to-use;
— Quality of service: fighting bureaucracy and long queues;
— Usefulness: addressing real everyday needs of the public and businesses;
— Completeness: all the services provided from one place (one-stop shop).

The strategy's legal grounds are:

— *Aqui communitaire* as of 2002;
— e-Signatures and e-Documents Act;
— e-Commerce Act;
— e-Communications Act;
— Implementing rules and regulations.

3 Status quo

There are a great number of independent e-Justice systems that already exist in Bulgaria. Such systems, for example, are:

— Court Case Management System (CCMS);
— Conviction Status Certificate System (CSCS);
— Bankruptcy Proceedings System (BPS);

— Unified Register System (URS);
— Legal Aid System;
— Enforcement of Judgments System;
— Mediators Register;
— Unified Information System to Counter Crime (UISCC);
— Bulgarian Citizenship Register;
— Commercial Register;
— BULSTAT Register;
— Property Register;
— Particular Pledge Register;
— Non-Governmental Organizations (NGO) Register;
— Political Parties Register;
— Judicial Statistics System.

All of these systems were created at different times, by different government agencies, are using different hardware and software, and are based on different standards.

4 Problems

The problems that the Bulgarian e-Justice faces can be divided into three main groups according to the number of pillars the strategy for e-Justice implementation in the country rests upon:

— Legal: lack of special material law, no procedural value of electronic documents;
— Technical: interoperability of systems created by different operators for different purposes;
— Operational: poor financing, bureaucracy, computer illiteracy on the part of civil servants and citizens.

5 The future

It is very hard to predict at this moment what the future holds for e-Justice in Bulgaria. Nevertheless, as a comprehensive, independent and self-sustaining system, it will, without doubt, comprise the following indispensable elements:

— The e-Justice Web Portal as the system's front end;
— Automated case management;
— Secure video communications/interrogations;
— e-Documents universal acceptance;
— B2B applications for legal professionals (prosecutors, notaries, bailiffs, etc.).

Ideally, over time, e-Justice in Bulgaria will become a paperless national justice system reliably serving interests of all the legal professionals in the country and the Bulgarian society at large.

CHAPTER 5

e-GOVERNANCE IN LESS ADVANCED STATES

THE NECESSARY ROLE OF e-GOVERNANCE IN THE SOCIO-ECONOMIC DEVELOPMENT. THE CASE OF TRANSITIONAL EU MEMBER COUNTRIES

Nicolae Costake[1]

Abstract

The development of the Information Society is a characteristic of the present socio-economic systems. One of the consequences is e-Government, a first step of e-Governance. The present paper discusses the content of Societal Management and expresses the view that e-Societal Management (e-SM), development of e-Governance, is one trend of the evolution of the Information Society. A societal management indicator is defined and used to suggest three clusters of the EU member countries. Transitional countries, subject in a greater measure to corruption, need higher rates of growth, which implies also e-SM. This aspect is detailed using the example of Romania, a typical transitional country. The specific priorities of the e-SM are described.

1 Statement of the Problem

The present paper discusses the necessary role of e-Governance in the socio-economic development, starting from the point of view that

1 Certified Management Consultant (by ICMCI), Bucharest, Romania, <ncp.costake@gmail.com>.

the improvement of the services of the public administration for citizens and businesses (e-Government) is just an initial improvement of governance. The development of covering also the outputs of the activities of the Judicial and Legislative Authorities considered as services can be named e-Governance, if based on the use of ICT (see e.g. [1], [2]). However, this is still a rather simplistic view, because it is not necessarily based on a relevant model of the socio-economic system (SES).

This paper is structured as follows: (i) the concept of societal management (SM); (ii) possible actions of the SM; (iii) the proposal of a simple criterion for classification of the performance of national SES, applied to the EU (this classification is used for identifying transitional countries); (iv) study case Romania and an exemplification Estonia–Romania; (v) conclusions for transitional EU member countries (EUMC). Due to the broad scope of the domain, the paper should be considered as one possible point of view.

2 Societal management

The concept of societal management is related to the concepts of society and management of socio-economic system. SM is an emerging system engineering discipline complementing the well established Enterprise Management (EM or Management of the Organization). EM is the management characterizing the operational subsystem, whereas SM is the management characterizing the societal management subsystem of the SES. The basic principles of management science apply to both EM and SM (e.g. the managerial functions). However, there are important differences, such as such suggested in Table 1.

Criterion	*Enterprise Management*	*Societal Management*
Scope	Organization or group organizations	Whole economic system
Success criterion	Profit	Socio-economic development (civilization)
Owners	Shareholders or similar (for public enterprises)	Stakeholders (in principle all citizens or tax-payers or electors)
Executive manager	Owner or nominated [and hired by the shareholders, if private enterprise]	Nominated, based on electoral results (political layer) or hired, based on competition (professional layer)
Customers	Target customers	All residents and organizations within the SES
Organizational characteristic	As decided by the management	Two-layered: (i) political; (ii) professional*
Delivery	Offer of products and services	Mandatory services (e.g. laws, basic educations, defense, etc.) and optional ones (e.g. which can be outsourced to the private sector)
Source of the power	Capital	Elections
Main aspects of power	Financial and knowledge power	Armed forces, authority and knowledge power
Main threat	a) Competition b) Poor business environment	a) Deterioration of the economy b) External dangers (e.g. terrorism) c) Deterioration of the environment
Danger of poor decisions	Limited to the existence of the enterprise and consequences to its direct stakeholders	Can be catastrophic for the own SES, possibly more
Success criterion	Profit, as large as possible, as quick as possible	Raising civilization, as well as possible, as quick as possible

Table 1. Enterprise Management versus Societal Management.

* Some state institutions are purely professional, requesting management's continuity (e.g. Statistics, Patent Office) or are incompatible with politics (e.g. Judiciary, Police, Army – why not Public Administration?).

The economic importance of SM is suggested by well known examples, such as, e.g.: (i) the post WW2 Marshall Plan; (ii) the growth of the Japanese and South Korean economies, in which public–private partnership played an important role; (iii) the big losses generated by the nazi governance in a hot world war and by the communist one in a cold one.

Globalization may generate contradictions between EM (tending to concentrate the economic activity in a reduced number of strong international companies which may become *de facto* monopolies) and SM (encouraging (i) development of the competition within the whole operational subsystem; (ii) compliance to the universal rights of people and (iii) the socio-economic development as a whole).

In SM, the decision can be (i) command–oriented (inducing changes supposed favorable in the operational subsystem) or (ii) adjustment–oriented (making use of the automatic circuits of the operational subsystem, enforcing or creating virtuous ones and minimizing the vicious ones). In both cases, decision relies on information and knowledge and only exceptionally on data. This implies the existence and performance of a societal feedback component of the societal management subsystem (adjustment–oriented SM implying a particular reliance on knowledge, in this case qualitative and mathematical models and democracy). Societal feedback is a component of the structure of the societal management subsystem (the legislative, judicial and executive authorities being complemented by a Societal Feedback Authority – SFA –) [3]. The autonomy of the SFA is important to assure the effect of continuous improvement based on democracy (electoral feedback and participation to decisions), official statistical information (tables, graphic and cartographic) and knowledge (*caeteris paribus* extrapolations and models) as well as audit (control of the respect of the law in collection and control of public money).

Due to the great complexity of the SES and the need of performance in societal decision-making, a multi-disciplinary system engineering

approach is needed. It implies the use of ICT. With other words, Information Society (IS) gives the possibility of performance in the societal management. EU is a large SES which is built by programs and projects to meet a general objective (vision): growth and employment in a society based on law and democracy, social cohesion, and on an economy based on free-market and competition, to be a major competitor on the world market. One can also keep in mind that every new society is the result of the technological progress (e.g. industrial after the agricultural one) that gives the possibility to its economy to increase the total value added per capita with at least one or two orders of magnitude. It follows that SM in the conditions of the IS (i.e. e-SM) should have a GDP target over 150 kEUR/capita, say.

The performance of SM (and e-SM) can be lowered by: (i) poor quality of the management of the state (such as: bureaucracy supported by rigid hierarchies; political influence beyond a thin layer of politically elected or nominated civil servants; political nominations without competence, insufficient MIS training); (ii) poor quality of the societal feedback, i.e. poor input for SM and EM decisions (it can be also due to lack of state's allocable or allocated resources); (iii) intoxication by power of high-ranked decision makers (lack of democracy); (iv) underground economy, i.e. economic transactions or industries which take place without any official financial or informational connection to the state. In this category, a range of situations can be found: from personal services paid without taxation till solid organized Mafia (collecting/producing/selling drugs or arms or offering high interest credits or other illegal services; its source of power is the capacity of punishment by crime and/or corruption); (v) corruption i.e. illegal administration of public service money or property against a personal advantage for a public servant (coruptee) and high advantages for the corruptor. It can be petty (underpaid civil servants accept pays for producing or delaying their tasks) but can become systemic (see e.g. [4]). It can reach the state in which law is ignored by stopping mandatory actions or deciding in the wrong sense. If this happens, there is a danger that the functioning of the

state is disturbed by law-making, investigation, judiciary and public administration and/or SFA entirely controlled by financially powerful 'groups of interests', cooperating with the members of Parliament, magistrates and civil servants, the election/nomination of which they control. This state can be characterized as 'total corruption'. The factors mentioned above are certainly influenced by imperfections of the SM. However, (iv) and (v) are illegal hence sensible to transparency. Transparency is supported by IS, e.g. by the minimization of using cash in conditions of e-Payment and e-Invoicing, unique identification of entities and integration of public information systems, etc., which can play a major role for effectiveness of the legislative and the other necessary measures. Reports on cost of corruption can be found. Some economic assessments take into consideration direct costs (such as the value of bribes), others are oriented on the general consequences, induced in the entire socio-economic system (SES). Examples in the first category are: ~3% of the worldwide GDP [reduction of taxations revenues in certain countries up to ~50% of the state budget [5]. Examples of the second category refer to up to 25% of the GDP [6] and even a reduction to more than 50% of the GDP [7] as a result of the development of a powerful underground economy.

3 Possible actions of the SM

Possible actions of the SM are exemplified in Table 2. Though simplified and simplistic, one can recognize the broad scope and high implications of societal management, as well as the importance of the Information and Communications Technology (ICT) support. This importance is increased by two high level autonomous factors: the accelerated technical and technological progress and the rapid deterioration of the environment. One conclusion is that governance by command cannot be recommended, because the model is too complex to be mastered by a single brain or a few brains.

Category	*Examples of products/services*	*Examples of ICT support*	*Comments*
Individual services for population and organizations	Recording and certifications of identities, relationships, states, events, rights, obligations, transactions between individual entities and the state. Assistance of paupers, disabled, urgent help in accidents and disasters. Protection of the individual and the property and other basic rights	Integration of the public information sharing common metadata, registers, information security management, co-operative networks, etc., making one-stop service feasible + societal feedback information system	e-Services
Products and services for groups of population and/or organizations	Education	Specific information systems integrated by sharing common information resources and exchanging information. Societal feedback information system, e-Libraries, e-Museums, e-CRM –Like system (examples of specific information systems) (*this structure applies to practical all following examples below*)	Including prescholar, primary, secondary including vocational, tertiary, post universitary
	Training unemployed/unemployable		
	Public health		
	Social security		
	Protection of basic rights		Such as e.g. preservation culture of ethnic groups
	Culture, sport, leisure		
Products and services for the entire population and all organizations	Enforcement of law and judicial decisions		
	Protection of public property		
	Protection of public order		

Category	*Examples of products/services*	*Examples of ICT support*	*Comments*
Products and services for the entire population and all organizations	Solving of conflicts and breaches of law	Definition of speci-fic performance indicators (e.g. avg. duration of cases and its components, uniformity of solu-tions) calculated using database/data warehouse & business intelligence technology	The specific integrated judicial information system supporting courts, investigating institutions (such as prosecutor offices) and penitentiaries following uniquely identified cases
	Public acquisitions and investments (may encourage e-Commerce, e-Business, e-Invoicing, e-Payments)	e-Procurement (may imply e-Market) and feedback (e.g. contract compared to ToR, final total cost and actual deadline compared with contract, client satisfaction, etc.	Oriented on socio-economic development and/or maximizing the ratio (performance/cost) of the public sector
	Public subventions (development decisi-ons for sectoral/territorial activities) (*Idem*)	Computer-aided modeling, improved by comparing (planned/actual states and trends) supporting impact studies before approval	Agriculture, R&D, public health are some usual examples
	Strategic planning of socio-economic development (sectoral / territorial)		Interface to world information is also necessary
	Public transport		The category and the environment deter-mines the necessary type of infrastructure and the public and private investments
	Public utilities		
	Public communications		
	Outsourcing activities and properties		See note below the table

Category	*Examples of products/services*	*Examples of ICT support*	*Comments*
Products and services for the entire SES	Laws, decrees, other normative acts, e-Democracy: organization, collection, processing and broadcasting of electoral feedbacks and of proposals, complaints and opinions from citizens and organizations, including by massmedia	Specific e-Legislative information system, supported by computer-aided modeling, improved by comparing (planned/actual states and trends) for impact assessment before approval	a) There are optimization aspects (great socio-economic influence). b) Must be complemented by civic information and education, to minimize manipulations by superior knowledge
	Public information (national and international)	Specific e-Democracy information system. Specific information system	e-Voting and official statistics are two examples
	Taxation (all kind of taxes and similar, tariffs and fees for public service), design, methodology and effective collection of current due debts, public financial inspection	• Financial and customs integrated information system (specific information system) • Financial inspection guidance information system based on business intelligence type processing of data in the information systems above	Encouraging e-Invoicing, e-Payment and switch from asking fiscal declarations towards asking confirmation or correction of draft declarations produced using existing information within the public information systems
	Regulation of the banking and insu-rance (provided by Central Banks) e.g. to keep inflation under control and protect against effects of bankruptcies in this market	• Generalization of e-Payments • Informatized financial management of banks and insurance companies • Use of financial models of the SES	
	• Administration and collection of profits from owned enterprises and other properties • Protection against financial losses due to current fiscal fraud, underground economy and corruption	• Public finance integrated information systems • Antifiscal fraud information system • Anticorruption information system	• Optimization aspects (great economic and social influence, e.g. supporting or reducing the development of middle-class) • Performance depending on the ICT systems integrated support

Category	*Examples of products/services*	*Examples of ICT support*	*Comments*
Products and services for the entire SES	Protection of the environment	• Public geographic information system (e.g. compliance to INSPIRE)	Affected by corruption and lack of education
	International relationships including trade, economical and political accords	• Interoperable information systems (e.g. pan European) • Standardized metadatabases • Public [multilingual] databases and data warehouses	
	Defense Anti-disaster protection (study, design, implementation, accumulation, maintenance)	Specific complex integrated information systems GIS-oriented	Imply that national information systems use common standards at least for metadata, communications, interoperability and information security management
Products and services specific to the IS (possible examples)	Shared knowledge	Knowledge bases shared by the judicial and legislative authorities	Supporting full coherence of legislative texts and judicial decisions and computer aided logical validation of drafts
	Multi-lingual translation	Automatic translation	Supporting interoperability
	New informational circuits	• Detected flaws in legislation by the Executive and Judicial Authorities sent for correction to the Legislative Authority • Introducing of finally results of judging frauds/crimes publishing the condemned into a public database	Creating or improving virtuous societal circuits or minimizing vicious ones
	Governance of SES oriented on minimizing differences between target and actual values of a set of KPI	• Macro socioeconomic dynamical model • Systematic determination of inertias and lags of the processes	

Category	*Examples of products/services*	*Examples of ICT support*	*Comments*
Products and services specific to transitional countries	Return of real estates to their true owners	• Electronic archiving of documents to ease one stop service	Real estates 'nationalized' by communist regimes
	Privatization of state – owned enterprises	• Public tendering information system[s]	Minimizing corruption
	EU funding management	• Specific EU funding management information system (permitting the use of electronic documents and archiving) • Program management of EU funds • Friendly web service support for documenting applications to obtain EU funding	The performance of these investments should meet not only local objectives, but also EU ones, as it involves public

Table 2. Actions of the state (examples).

Note: Provided that the long-term general interest is not affected by short-term local interest and higher performance supported by impact studies before submitting for approval and the activity is accountable and guaranteed by periodic and transparent evaluations, public activities can be transferred to the private sector or public–private partnership organizations.

The possible actions of the SM are defined in the Constitutions, voted by the population. Apart emergency situations, the SM actions imply: (i) strategic planning; (ii) decision (preceded by new information, elaboration including impact assessment); (iii) implementation; (iv) response of the target socio-economic processes; (v) possible corrective or improving actions. The whole cycle takes place in the conditions of responses from other socio-economic processes (indirectly influenced by the decision) and possible disturbances generated by the international environment and the underground economy. It results that SM implies very high responsibilities and competences (to find the good balance between prudence and need to move fast in the global economy) and a solid support of professional civil servants to assure the necessary continuity in the condition of periodical change of political executive managers.

4 Societal management performance. Example of the EU

Apart official statistics, there is a large literature on indicators for socio-economic systems. The definition of a simple key performance indicator (KPI) roughly characterizing the level of the SM and based on easy accessible data can be useful. A 'societal management index' was proposed (e.g. [3]) as:

$$\text{SMI} = \frac{\text{GDP/capita [kEUR]}}{\text{Unemployment rate [\%]}} \times \text{(Corruption Perception Index)}$$

Statistical data provided by the European Information Technology Observatory [8] and the e-Government Observatory [9] of the European Commission (EC) can be used. As it is a qualitative study, data can be rounded, characterizing orders of magnitude. (Of course, one must take into consideration also that some indicators have different dynamics – e.g. the growth or decrease of the population is usually slower than that of the rate of growth of the GDP, at least in the European context.)

The calculations for the 27 EU member countries (EUMC) (see Annex A), suggest that three clusters of countries can be recognized:

a) The transforming countries (Bulgaria, Czech Republic, Greece, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia). Their average SMI value is ~3 kEUR/capita. They account for ~23% of the population (average unemployment rate ~11.7%) and ~8% of the European GDP. They spent ~6% of the GDP for ICT expenditures. One key problem seems to be the high (perhaps systemic) corruption (average CPI value: ~4.6).

b) The main group of countries (Belgium, Cyprus, Estonia, France, Germany, Italy, Malta, Portugal, Slovenia, Spain). Their average SMI is ~19 kEUR/capita. Their population is ~55% of the EU, producing 61% of the European GDP, with an unemployment rate of ~8.9%. Their expenditures for ICT amounts to ~9% of the GDP.

The average value of the CPI is ~6.6. Their main problem seems to be the increase of the GDP's growth rates. However, the more recent figures (in 2007) show important increases of the values corresponding to large countries (such as France and Germany).

c) The advanced countries (Austria, Denmark, Finland, Ireland, Luxemburg, The Netherlands, Sweden, United Kingdom). Their average value of the SMI is ~54 kEUR/capita. They represent ~22% of the population and generate ~31% of the GDP with an unemployment rate of ~5%. They spent ~14% of their GDP for ICT expenditures. Their average value for CPI is ~8.8.

One of the consequences of this situation, is the differentiation of requirements concerning the SM, if social the cohesion should be improved in less than a generation. For the advanced EUMC it is a normal evolution towards e-SM and its advantages. The main group of EUMC would probably accelerate their growth by incorporating best SM and ICT practices, supported also by EU financed projects. For the transitional countries the problem is more complicated because of (i) the losses due to underground economy and corruption which oppose good governance; (ii) the need to accelerate the annual rate of GDP over ~10% in order to meet the normal EU level. It also results that the concept of e-Inclusion could perhaps be considered at two levels: (i) at the individual and organization level; (ii) at SES level. With other words, e-SM should become accessible to all SES of the EUMC.

5 EU and e-SM

One can notice that the development of e-Government and of using ICT in the activities of the EU, goes towards e-SM, even if no formal e-SM strategic planning exists. The attention is now on reducing the administrative burden for the businesses (and citizens) by duplications in reporting information elements to the state, which could lead to reduction of costs of ~5% of EU's GDP [10],

together with e-Procurement of public acquisitions, which could lead to economies of ~1% of EU's GDP [11]. e-Commerce and e-Business will be better supported by generalizing e-Invoicing (see e.g. [12]), e-Payments ([13], [14]), development of interoperability in the sense of accepting in administrative and legal processes documents produced in the EU countries [15] and, indirectly, by one-step services. It is also supported by (i) the development of European Information Space based on next-generation broadband networks supporting the rapid development of European content industry and services, (ii) new initiatives [16], [17] and the elaboration of conceptual solutions, collections of best practices and standards for European public information systems in the European information space (e.g. [18] to [20]). One can still notice the focus on the Executive Authority (in the classical sense of the model of 3 Authorities). However, the increasing use of mathematical models as a support for European economic decisions, such as e.g. in the field of structural funds (e.g. [21]) is also a signal for the Legislative Authority. Legislation and Judiciary are considered in the framework of the LEFIS project, a component of the SOCRATES program. (Proposals related to the societal management aspect were presented at Wroclaw and Zaragoza workshops.)

6 Problems of transitional EU countries

6.1 Case Study Romania

The statistical data suggest that Romania can be considered representative for the transitional EUMC. Romania acceded to the EU at January, 1st 2007 but a pre-accession report [22] and a post accession one [23] state issues to be solved (see Table 3).

Pre-accession general issues	*Post accession general issues*
Limited progress in the reform of public administration	No special mention
Legislative framework to be completed regarding: • financing of the political parties • verification of wealth declarations • verification of conflicts of interests • liability of public persons	Establishment of an integrity agency for verifying assets, potential conflicts of interest and issuing dissuasive anti-fraud actions
Parliament to demonstrate clear political will in long-term fighting against high-level corruption	Overall, progress in the judicial treatment of high-level corruption is still insufficient
Current investigations into high-level corruption should lead to criminal trials, final convictions and dissuasive sentences in a reasonable timeframe	A more transparent and efficient judicial process by enhancing the capacity and accountability of the Superior Council of Magistrates. Design and implemention of a rational and realistic staffing model for the justice system. Develop and implement a plan to re-structure Public Ministry addressing the managerial shortcomings and HR issues. Monitor the impact of the amendments to Civil and Criminal Procedure Code. Further measures to prevent and fight against corruption, in particular for local governments
Urgent measures to manage: excess occupancy and e-Sanitary facilities in psychiatric institutions; mental health care in communities; access to pharmaceuticals. Ensure new strategy for disabled and for quality of residential institutions. Improve Roma's conditions on the ground and combat discriminations. Government revenue (in terms of proportion of GDP) remains low. Accumulation of bad debts remains high. Privatization is progressing at low pace. Acceleration needed for the integrated administration and control system	No special mention
Acceleration needed for administrative capacity to manage EU funds	Hard to assess in absence of analytical instruments

Table 3. Romania's pre and post EU accession issues as reported by the EC.

One may notice that performance of the judiciary, administrative capacity and corruption are considered as problems. A recent letter of the EC [24] regarding persisting shortcomings of the integrated administration and control information system and insufficient

quality of the land parcel identification system inaugurates the threat to diminish by 25% the European financial support caused by a poor component of the SM (in the field of agriculture).

6.2 Estonia versus Romania

One could continue by describing Romania's problems, but this would mean a considerable volume (a start can be found in [25]). Instead, a simple analysis of the comparison with Estonia, the country having the highest SMI value of the former Eastern European states part of the 'Socialist Block' headed by the Soviet Union, can be considered to be relevant. Recent data (April 2007) from EC's e-Government Observatory factsheets are used. The historical backgrounds, the initial 1989 states and the evolutions of the two countries are different. A selection of indicators are presented in Table 4.

Indicator	*Estonia (EE)*	*Romania (RO)*
Population [M inhabitants, 2006]	1.3	21.6
GDP [M EUR market prices, 2005]	14000	79551
GDP/capita (from above) [kEUR]	10.8	3.7
GDP growth rate [%]	11.4 (2006)	4.1 (2005)
Inflation rate [%, 2006]	4.4	6.6
Unemployment rate [%, 2006]	5.9	7.4
Government debt/GDP [%, 2005]	4.5	15.2
Households with Internet access [%]	46 (2006)	6 (2004)
Enterprises with Internet access [%, 2004]	90	52
Enterprises with broad-band connection [%]	76 (2006)	7 (2004)
Enterprises having received orders on-line in the previous year [%, 2006]	14	Data not reported
e-Services for citizens [%]*	~80	~40
e-Services for businesses [%]*	~100	~65

Table 4. A selection of indicators for Estonia and Romania.

* The values of the e-Services are uniformitized: (i) the values of the e-Services are considered as the maximal levels declared; if the maximum value is 3 then it is multiplied by 4/3, independent of the administrative or outsourced body.

Other comparation criteria using data contained in the EC's e-Government Observatory Factsheets are:

(i) e-Government strategy. Estonian Information Society Strategy 2013 (entered into force in January 2007). In Romania it is a section of the Government program 2004-2008.

(ii) Government legal framework. In Estonia: Personal data protection (1996); Databases (1997); Identity documents (1999); Public information (2000); Digital signatures (2000); Public procurement (2000); Information Society services (2004); Electronic communications (2004). In Romania: Public information (2001); e-Signature (2001); e-Commerce (2002); e-Payment of local taxes (2002); Access to e-Communications networks (2002, 2003); Information services (2003); Personal data protection (2004); (e-Procurement law exists, but is not mentioned).

(iii) e-Government actors – national. In Estonia: Ministry of Economic Affairs and Communications (MEAC): policy/strategy and coordination (via RISO Dept.); RISO and Estonian Informatics Centre (RIA): development and implementation of government wide inform. systems and main components of e-Government. infrastructure; Ministries and Agencies: departmental projects. RISO and RIA: support National Audit Office (NAO): promotion of reform and support to public bodies for best value for taxpayers; Certification Authority: certification of ID cards digital signatures; e-Governance Academy: training of civil servants, policy makers and representatives of civil society; Estonian Association of ICT: cooperation of the ICT industry and educational institutions; Estonian Association of ICT: cooperation of the ICT industry and educational institutions; Estonian IT Foundation: support for national ICT development. In Romania: Ministry of Administration and Interior (MAI): main e-Government user and policy contributor; Ministry for Communications and Information Technology (MCIT): main policy and strategy producer, coordination of the implementation of policies and strategies along with subordinated agencies and departments; the General Inspectorate for CIT (recently transformed into a National Agency):

overall supervision + responsibility for 3 portals: e-Government, e-Procurement, vehicle registration and permits; MCIT: knowledge-based economy project (World Bank loan) management unit: supports disadvantaged communities in knowledge economy and society; National Regulatory Authority for CIT: instituional IT regulatory framework including harmonization with the EU legislation, promoting competition, protection of the interest of end-users, encouraging investments in infra-structure; MCIT through private sector contractors: implementation, support.

(iv) e-Government actors – regional and local. In Estonia: Ministry for Internal Affairs (MIA): drafting IS program and action plan for municipalities and implementation; MIA, Population register, RIA, RISO, NAO: support, audit; Association of cities, and of municipalities: representing interests and arranging cooperation. In Romania: No specific information reported (de-centralized state bodies are subordinated to the central public authorities, local informatization actions are in the competence of the local authorities).

(v) e-Government infrastructure. In Estonia: e-Government portal; EE Bone (broadband communications network between government institutions); e-ID card; free use common digital signature system; mobile ID; e-Passport; public procurement state register; X-Road middleware (communication between databases); administration system of the state information system (includes the state register of databases); electronic document exchange center. In Romania: No specific information reported (not even the 'Special Telecommunication Service' administrating and running the TESTA compatible VPN connecting institutions of state public administration).

One may notice that Romania did not adopt an updated Strategy for Information Society. An analysis of the legislative dynamics shows in Romania a large flow of normative acts and a high ratio of the number of Government ordinary and emergency ordinances (OO, EO) versus number of laws. This may suggest a trend towards

'governance by command'. It is also rather strange that the Law 260/2007 (July) for electronic recording of commercial transactions does not refer to the i2010 Program and/or EU Directives.

The evolutions of the CPI [26] is shown in Table 5 (rounded values).

Though there are similarities in the two dynamics, it is obvious that Romania must increase the anti-corruption effort. One can also conclude that Romania encounters societal management problems,

Country	*Estonia (EE)*	*Romania (RO)*	*EE/RO*
1998	5.7	3.0	1.9
1999	5.7	3.3	1.7
2000	5.7	2.9	<2.0
2001	5.6	2.8	2.0
2002	5.6	2.6	2.2
2003	5.5	2.8	<2.0
2004	6.0	2.9	2.1
2005	6.4	3.0	>2.1
2006	6.7	3.1	<2.2
2006/2003	1.2	1.1	

Table 5. Evolution of the Corruption Perception Indexes of Estonia and Romania.

whereas the evolution of Estonia towards the Information Society relies on a solid societal management foundation.

7 Specific problems for a Strategy for Starting Sustainable Accelerated Socio-Economic Growth

The problem for starting acceleration of a sustainable socio-economic growth is to assure high-quality governance decisions. This implies (i) a proper Societal Management organizational structure; (ii) a corresponding support; (iii) a development strategy starting with prioritization of e-Governance actions (including (i) and (ii)). Such a point of view was expressed [27].

However, a strategy can be jeopardized if problems occur in the informational content coherence, if legislation is not calm and in line with those of the EU, if police and justice do not perform their homeostatic role (to solve quickly and accurately breaches of law), if societal feedback is not accurate and complete, or if the state does not collect the necessary money to implement and develop the necessary information system or the quality of the societal feedback is poor.

The necessary technical support is suggested in Fig. 1 below.

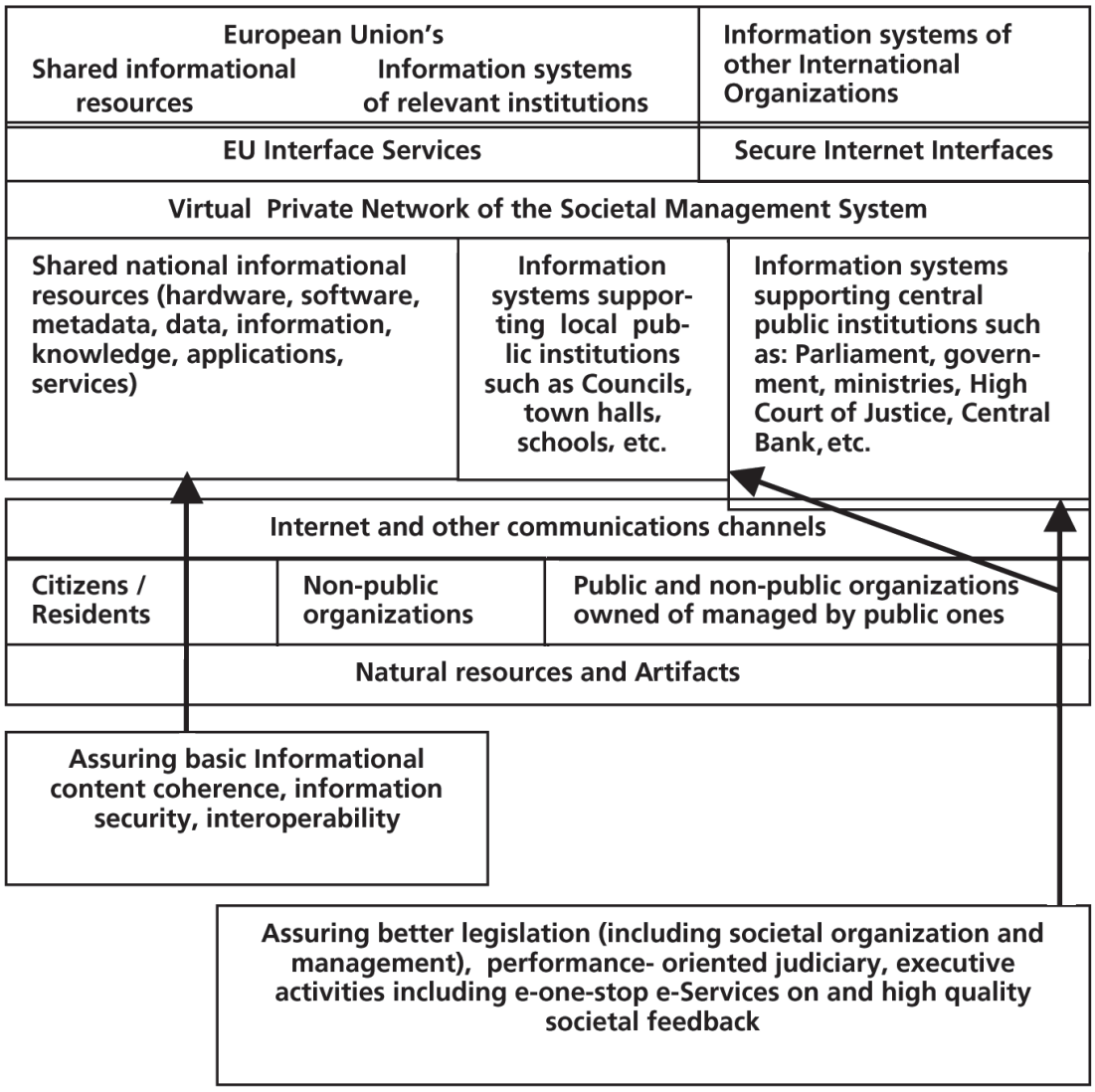

Fig. 1. A model of the technical support for e-SM.

It includes: (i) a cooperative ICT infrastructure (such as pan-European connected public networks and flexible service oriented architecture applications for public information systems); (ii) an informational coherence kernel (shared metadata, registers and/or data bases of the basic entities of the SES, knowledge bases (including definition of concepts, standards, processes and procedures) and shared standardized applications of general interest). This ensures the unique identification of the basic entities of the SES and the coherence of the informational content; (iii) precise definitions of targets (including KPI), roles and responsibilities of the state institutions (and their permanent working committees), in the horizontal and vertical coordinates. One issue, to be cleared by the European Constitution, is the definition of targets and of the delegation of authority between countries and EU; (iv) permanent improving and development, which is a component of quality assurance. The assurance of the quality of the legislative information system requires: (i) a shared judicial and legislative knowledge base for definitions of concepts and standardized specific metadata and procedures; (ii) a centralized case database shared by courts, prosecuting/investigating organizations and penitentiaries; (iii) a data warehouse for calculating KPI referring to durations and degree of consistency of the judicial solutions.

The quality assurance of the financial information system refers to: (i) one-stop e-Services to natural and legal tax payers; (ii) minimization of losses for the state's revenues (such as e.g. improvement of taxation regulations and of collection & control techniques; computer aided public acquisitions enhanced by follow-up the performance of the contracts and stakeholders satisfaction opinion surveys); (iii) optimization of taxation rules taking into account the economy's growth and consequences on consumer market and social cohesion as well the growth or involution of the middle class; (iv) minimization of cash transactions by generalizing e-Invoicing and e-Payment in the relationship with public institutions; (v) centralized standard web services-based information system for managing international funding; (vi) gradual integration of the public information systems in order to switch from

declarations asked from the natural and legal taxpayers to draft declarations sent to the taxpayers for confirmation/modification.

Improvement of the statistical information system is needed in order to meet the requirements, including interfacing with the various information systems of the SES and Eurostat, and production and updating of models in supporting governance decision-making processes.

For the transitional countries, the first priorities appear to be:

a) The selection of a solid organizational owner (e.g. a national CIO of the Prime Minister, Ministry of Finance or Ministry of Interior) and the adoption of a vision and strategic planning, based on the model of Fig. 1.

b) The creation of the mandatory informational infrastructure for coherent actions of the public sector, including one-stop e-Services to citizens and businesses, e-Payment and e-Invoicing, using EU standards and recomendations. Nomenclatures data base, population, organizations and real estates register and public sector VPN.

c) Development of integrated information systems for: (i) public acquisitions (including protection against inacceptables offers – such as competition between companies controlled by the same owner and post-contractual feebdack such as actual costs and benefits and stakeholder's satisfaction); (ii) taxation, tax collection, management of international fundings; (iii) informization of the legislative process and its quality assurance, for EU compatibility; (iv) informatization of the judicial investigation and judgement process, calculating key performance indicators; (v) accurate and reliable official societal feedback provided by the official statistics, citizen's electoral decisions and their participation to governance decisions.

Integrated information systems assuring both e-Services including e-Procurement, correct taxation (and tax collection), effective management of international funding, good legislation, correct and performant judgement and good societal feedback permit the increase of the administrative capacity to the level necessary in the Information Society.

8 General Conclusions

Following general conclusions are proposed:

a) In the EU's socio-economic system three clusters can be identified. In particular, for the cluster of transitional countries the acceleration of the socio-economic development is a vital requirement. This implies e-SM.

b) For the said cluster, specific strategic planning and follow-up, integrated in the EU's development strategy is necessary. The prioritization of the objectives is also necessary.

Annex A

Examples of values of the proposed societal management index

Country	*GDP/capita [kEUR]*	*(GDP/capita [kEUR]) Unemployment rate [%]*	*SMI: (GDP/capita [kEUR] Unempl. rate [%])* CPI*
Luxemburg	58.0	12.9	110.8
Denmark	38.5	8.0	76.2
Ireland	38.3	8.7	64.5
The Netherlands	31.0	6.6	57.5
United Kingdom	31.3	6.5	56.1
Austria	29.9	6.2	53.5
Sweden	32.0	4.1	37.7
Finland	30.2	3.6	34.5
Belgium	28.5	3.4	24.7
Germany	27.2	2.9	22.9
France	27.2	2.7	20.3
Cyprus	17.7	3.6	20.2
Spain	20.7	2.4	16.4
Slovenia	15.0	2.5	16.0
Italy	24.2	3.1	15.4
Portugal	14.8	1.9	12.7
Estonia	10.8	1.8	12.2
Malta	11.3	1.5	9.9
Greece	16.3	1.7	7.3
Czech Republic	9.7	1.3	6.5
Hungary	8.8	1.2	6.1
Latvia	7.0	1.0	4.9
Lithuania	6.2	0.7	3.6
Slovakia	7.0	0.4	2.0
Romania	3.7	0.5	1.6
Poland	6.4	0.4	1.3
Bulgaria	2.7	0.3	1.2

References

[1] Costake, N., 'From e-Government to e-Governance', in A. V. Antiroikko and M. Malki (eds.), *Encyclopedia of Digital Government Section F,* Hershey, PA (USA): Idea Group.

[2] Finger, M., and G. Pécoud, 'Towards a model of e-Governance', *EJEG*, 1 (2003), <http://www.jpeg.org>.

[3] Zahan, E., and N. Costake, 'Priorities for e-Government in European Transforming Countries. The Example of Romania', in *Proceedings of ICEG 2007* (*University of Quebec Montreal, Canada*), pp. 331–40.

[4] Pope, T. I., *The TI Source Book 1999: National Integrity System Transparency International*, Berlin, 1999, <http://www.transparency.org/>.

[5] Cobb, S. (US Ambassador), 'Price of corruptio', *Remarks at the Meeting of American Chamber of Commerce in Kingston, Jamaica, March 2003*.

[6] Transparency International Kenya, 'Cost of Corruption', *ADILI*, no. 89 (April 2007).

[7] Salisu, M., 'Corruption in Nigeria', Lancaster University Management School Working Paper 2000/006, <http://www.lums. co.uk /publications>.

[8] European Information Technology Observatory, <http://www.eito.org>.

[9] e-Government Observatory: <http://europa.eu.int/comm>, Information Society > IDABC > epractice.eu > Library Documents.

[10] Reding, V., 'The political challenge of simplifying and opening up e-Government', Speech delivered to the International Conference *Advancing e-Government*, Berlin, March 2007.

[11] Timmers, P., 'The impact of e-Government', <http://217.59.60.50/eGEP/Static/E_FWorkshop_II.asp?ST=0&page=1>.

[12] Engel-Flechsig, S., 'Electronic invoice solutions in Europe', *Workshop on electronic invoices*, II ppt (June 2007).

[13] Central European Bank, *The single euro payment area (SEPA). An integrated retail payment market*, Frankfurt a. M.: European Central Bank, 2006.
[14] Central European Bank, 'Guideline on a Trans-European automated real-time gross settlement express transfer system (TARGET)', 30 December 2005 ECB/2005/16 (2006/21/EC).
[15] EC, *Interoperable delivery of pan-European Services to Public Administration, Businesses and Citizens* (Decision 2004/387/EC).
[16] Reding, V., 'i2010 – 2 years on', Speech delivered to the General Assembly of the European ICT Association Brussels, May 2007.
[17] Reding, V., 'Enhancing information security in software and services. What role for government, security providers and users?', Speech delivered at the European Information Security Awareness Day Brussels, February 2007.
[18] EC, *Convergence of Communications Technology, Media and information Technology* (COM 97/0623/final).
[19] EC, 'IDA Architectural guidelines', <http://ec.europa.eu/idabc/en/document/3485/5585>.
[20] EC, 'INSPIRE (Infrastructure for Spatial Information in Europe)', <http://www.ec-gis.org/inspire/>.
[21] Bradley, J., et al., 'HERMIN. A macroeconometric modelling framework for the EU periphery', *Economic Modelling*, vol. 12, no. 3 (1995).
[22] EC, *Monitoring Report on the state of preparedness for EU Membership of Bulgaria and Romania*, Brussels, September 2006 (COM, 2006).
[23] EC, *Report on Romania's Progress accompanying Measures following Accession XXX Brussels, June 2007*, <http://www.infoeuropa.ro>.
[24] European Commission, *Commission gives one month to improve farm aid systems, welcomes progress made in Bulgaria*, <http://www.infoeuropa.ro/docs/IP-07-1474_RO EN.pdf>.
[25] Costake, N., 'A system engineering problem: Informatized Societal Management', in *Leonardo da Vinci 7th European Conference,* E Comm Line Bucharest, 2006. (These proceedings have no pagination.)

[26] Transparency International, 'Surveys and Indices', <http://www.newsnfo.co.uk/pages/2005%20-%20cpi%20-%20surveys_indices%20-%20policy_research%20-%20home%20-%20Transparency %20International.htm>.
[27] Costake, N., and F. Galindo, 'A strategy for e-Governance Fortune', *Journal for International Management*, vol. 1, special issue (January–June 2005), pp. 67–89.